PCT/JP00/05742
09/830392

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 12 SEP 2000
WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

JP00/05742
EKU

出願年月日
Date of Application: １９９９年　８月２７日

出願番号
Application Number: 平成１１年特許願第２４２２９４号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２０００年　６月２９日

特許庁長官
Commissioner,
Patent Office

近藤隆彦

出証番号　出証特２０００－３０４９７２６

【書類名】　特許願

【整理番号】　9900471511

【提出日】　平成11年 8月27日

【あて先】　特許庁長官　伊佐山　建志　殿

【国際特許分類】　H04L 12/16

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内

【氏名】　大石　丈於

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内

【氏名】　松山　科子

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内

【氏名】　浅野　智之

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内

【氏名】　武藤　明宏

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内

【氏名】　北原　淳

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082740

【弁理士】

【氏名又は名称】　田辺　恵基

【手数料の表示】

【予納台帳番号】　048253

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9709125

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報送信システム、情報送信装置及び情報受信装置

【特許請求の範囲】

【請求項１】

データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対する署名を生成して上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信し、

上記データ受信装置は、

上記署名の検証を行うと共に、上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成者識別データとを比較する

ことを特徴とする情報送信システム。

【請求項２】

データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対する署名を別々に生成して、当該生成されたデータ用署名及び取扱方針用署名を上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信し、

上記データ受信装置は、

上記データ用署名及び上記取扱方針用署名の検証を行うと共に、上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成者識別データとを比較する

ことを特徴とする情報送信システム。

【請求項３】

データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、

上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を生成して上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信し、

上記データ受信装置は、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする情報送信システム。

【請求項４】

データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータに対するデータ用署名を生成すると共に上記取扱方針データ及び上記データ用署名に対する取扱方針用署名の生成を行い、上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を上記データ受信装置に送信し、

上記データ受信装置は、上記データ用署名及び上記取扱方針用署名の検証を行う

ことを特徴とする情報送信システム。

【請求項５】

データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針

を記述した取扱方針データを生成し、上記取扱方針データに対する取扱方針用署名の生成と、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名を生成し、上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を上記データ受信装置に送信し、

上記データ受信装置は、上記データ用署名及び上記取扱方針用署名の検証を行う

ことを特徴とする情報送信システム。

【請求項６】

上記情報送信システムは、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化鍵データに対する鍵データ用署名を生成し、当該生成された鍵データ用署名を上記データ受信装置に送信し、

上記データ受信装置は、上記鍵データ用署名の検証を行う

ことを特徴とする請求項１、２、４又は５に記載の情報送信システム。

【請求項７】

上記情報送信システムは、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化されたデータ、上記暗号化鍵データ及び上記取扱方針に対するセキュアコンテナ用署名の生成を行い、上記暗号化されたデータ、上記暗号化鍵データ、上記取扱方針データ及び上記セキュアコンテナ用署名を上記データ受信装置に送信し、

上記データ受信装置は、上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求項３に記載の情報送信システム。

【請求項８】

所定のデータをデータ受信装置に送信する情報送信装置において、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対する署名を生成して上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信する

ことを特徴とする情報送信装置。

【請求項９】

所定のデータをデータ受信装置に送信する情報送信装置において、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対する署名を別々に生成して、当該生成されたデータ用署名及び取扱方針用署名を上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信する

ことを特徴とする情報送信装置。

【請求項１０】

所定のデータをデータ受信装置に送信する情報送信装置において、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、

上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を生成して上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信する

ことを特徴とする情報送信装置。

【請求項１１】

所定のデータをデータ受信装置に送信する情報送信装置において、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータに対するデータ用署名を生成すると共に上記取扱方針データ及び上記データ用署名に対する取扱方針用署名の生成を行い、上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を上記データ受信装置に送信する

ことを特徴とする情報送信装置。

【請求項１２】

所定のデータをデータ受信装置に送信する情報送信装置において、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記取扱方針データに対する取扱方針用署

名の生成と、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名を生成し、上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を上記データ受信装置に送信する

ことを特徴とする情報送信装置。

【請求項１３】

配送用の鍵データで暗号化された所定のデータを含む送信データを情報送信装置から受け取る情報受信装置において、

予め与えられている上記鍵データを用いて上記データを復号する

ことを特徴とする情報受信装置。

【請求項１４】

コンテンツ鍵で暗号化された所定のコンテンツデータを含む送信データを情報送信装置から受け取る情報受信装置において、

上記コンテンツ鍵で暗号化された上記コンテンツデータと共に上記情報送信装置から配信される、個別鍵で暗号化された上記コンテンツ鍵及び配送鍵で暗号化された上記個別鍵を受信し、予め与えられている配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵で上記コンテンツデータを復号する

ことを特徴とする情報受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報送信システムに関し、コンテンツ保有者又は販売者が、コンテンツを安全にコンテンツ利用者に配送し得る情報送信システムに適用して好適なものである。

【０００２】

【従来の技術】

音楽などの情報（コンテンツ）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザがその情報処理装置でコンテンツを復号して、利用するシステムである。

【０００３】

例えば図９１に示すように、２つのコンテンツ送信装置および１つのコンテンツ受信装置が設けられている場合について説明する。

【０００４】

第１のコンテンツ送信装置３００は、データ暗号部３０１、データ暗号部３０２、コンテンツ鍵生成部３０３、耐タンパメモリ（Tamper Resistant Memory）３０４を有している。なお、ここで言う耐タンパメモリとは、第３者に容易にデータを読み出されないものであればよく、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。耐タンパメモリ３０４にはコンテンツ鍵（Content Key）K_{co}を暗号化するのに必要な配送鍵（Distribution Key）K_dが、予め電子配信サービスセンタ（図示せず）から供給され、保存されている。

【０００５】

コンテンツ送信装置３００は、コンテンツ受信装置３２０に渡すデータを生成するため、コンテンツ鍵生成部３０３を用いてコンテンツ鍵K_{co1}を生成し、この鍵を用いてデータ暗号部３０１にてコンテンツを暗号化する。また、コンテンツ鍵K_{co1}はデータ暗号部３０２にて配送鍵K_dを用いて暗号化される。これら暗号化されたコンテンツおよびコンテンツ鍵K_{co1}がコンテンツ受信装置３２０に送信される。

【０００６】

因に、第２のコンテンツ送信装置３１０は、コンテンツ送信装置３００と同様にして、データ暗号部３１１、データ暗号部３１２、コンテンツ鍵生成部３１３、耐タンパメモリ３１４を有し、コンテンツ鍵生成部３１３においてコンテンツ鍵K_{co2}を生成し、この鍵を用いてデータ暗号部３１１によりコンテンツを暗号化する。またデータ暗号部３１２は電子配信サービスセンタ（図示せず）から供給される配送鍵K_dを用いてコンテンツ鍵K_{co2}を暗号化する。かくして第２のコンテンツ送信装置３１０は、暗号化されたコンテンツ及び暗号化されたコンテンツ鍵K_{co2}をコンテンツ受信装置３２０に送信する。

【０００７】

コンテンツ受信装置３２０は、送受信部３２１、上位コントローラ３２２、暗号処理部３２３、メモリ３２４、データ復号部３２５、データ復号部３２６、耐タンパメモリ３２７を有する。なお、コンテンツ利用者が不特定多数であり、コンテンツ利用者が機器をどのように扱うか把握できないため、ここで言う耐タンパメモリとはハードウェア的に内部データが保護される必要性があり、従って暗号処理部３２３は、外部からアクセスしにくい構造を持った半導体チップで、多層構造を有し、その内部の耐タンパメモリはアルミニュウム層等のダミー層に挟まれ、また、動作する電圧及び又は周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する。そして、耐タンパメモリ３２７には、電子配信サービスセンタ（図示せず）から予め供給された配送鍵K_dが保存されている。

【０００８】

因に、コンテンツ送信装置３００及び３１０の耐タンパメモリ３０４、３１４は、外部からアクセス可能なメモリであるが、そのアクセス方法に制約を設けている。それがパスワードであったり、入室管理であったりする。一方、コンテンツ受信装置３２０の耐タンパメモリ３２７においては、メモリそのものが外部から不正にアクセスされない構造を有し、正規のアクセス手段で外部から内部データを読み出す方法も限定されているか、全くない。なお、耐タンパメモリ３２７は外部からその内部データを読み出すことは全くできないが、以前の鍵データ等を用いれば、外部からデータの変更のみできるアクセス方法がある場合がある。また、暗号処理部３２３内では、メモリにアクセスして所定のデータを読み出すことができるのに対して、外部から内部のメモリを読み出すことができないようになされている。

【０００９】

コンテンツ送信者３００または３１０から送信されてきたコンテンツおよびコンテンツ鍵K_{co1}及びK_{co2}は、送受信部３２１で受信され、上位コントローラ３２２に引き渡される。上位コントローラ３２２は、これらのデータをいったんメモリ３２４に保存し、コンテンツを利用する場合には、コンテンツ鍵K_{co}、コ

ンテンツを暗号処理部３２３に引き渡す。これを受信した暗号処理部３２３は、データ復号部３２５で予め耐タンパメモリ３２７に保存しておいた配送鍵K_dを用いて復号化し、引き続きコンテンツをデータ復号部３２６でコンテンツ鍵K_{co}を用いて復号化し、コンテンツを利用する。この時、課金処理を伴う場合がある。

【００１０】

【発明が解決しようとする課題】

しかしながら、図９１に示す従来の情報処理システムにおいては、コンテンツ送信装置３００および３１０が同一の配送鍵K_dを使用しているため、互いにコンテンツ情報を盗み取ることができる問題があった。この問題点を解決するための一つの方法として、コンテンツ送信装置毎に異なる配送鍵K_dを使用することにより送信装置相互のコンテンツ情報の盗用を防止する方法が考えられる。ところが、この場合、コンテンツ受信装置が全ての配送鍵K_dを保持しておく必要があり、この分受信装置の構成及び受信方法が煩雑になる問題があった。

【００１１】

【課題を解決するための手段】

上記課題を解決するため本発明においては、情報送信装置は、コンテンツデータを所定のコンテンツ鍵で暗号化すると共に、情報送信装置固有の個別鍵で上記コンテンツ鍵を暗号化し、コンテンツ鍵で暗号化されたコンテンツデータと、個別鍵で暗号化されたコンテンツ鍵と、所定の配送鍵で個別鍵を暗号化してなる外部から供給された暗号化個別鍵とを情報受信装置に送信し、情報受信装置は、予め与えられている配送鍵で個別鍵を復号し、当該復号された個別鍵でコンテンツ鍵を復号し、当該復号されたコンテンツ鍵でコンテンツデータを復号する。

【００１２】

複数の情報送信装置は、配送鍵を持たないことにより、互いにコンテンツデータの盗用を防止することができる。そして情報受信装置は、１種類の配送鍵を持つだけで複数の情報送信装置からのコンテンツを復号することができる。

【００１３】

【発明の実施の形態】

以下、図面について本発明の一実施の形態を詳述する。

【００１４】

（１）情報配信システム

図１は、本発明を適用したEMD(Electronic Music Distribution ：電子音楽配信）システム１０を説明する図である。このシステムでユーザに配信されるコンテンツ（Content ）とは、情報そのものが価値を有するディジタルデータで、この例の場合、１つのコンテンツは、１曲分の音楽データに相当する。コンテンツは、１つのコンテンツが１つの単位（シングル）として、または複数のコンテンツが１つの単位（アルバム）としてユーザに提供される。ユーザは、コンテンツを購入し（実際には、コンテンツ鍵K_{co}を利用する権利を購入し）、提供されるコンテンツを利用する（実際には、コンテンツ鍵K_{co}を用いてコンテンツを復号化し、利用する）。なお、勿論、音楽データだけでなく、映像、ゲームプログラム等、コンテンツの販売全てに適用可能である。

【００１５】

電子配信サービスセンタ（END Service Center）１は、コンテンツプロバイダ（Content Provider）２に個別鍵K_i、コンテンツプロバイダ２の公開鍵証明書を送信し、サービスプロバイダ（Service Provider）３にサービスプロバイダ３の公開鍵証明書を送信し、ユーザホームネットワーク５に対しては配送鍵K_dや登録情報を送信し、ユーザホームネットワーク５から、コンテンツの利用に応じた課金情報等や登録情報を受信し、課金情報に基づいて利用料金を精算し、コンテンツプロバイダ２、サービスプロバイダ３および電子配信サービスセンタ１自身へ利益分配の処理を行う。

【００１６】

コンテンツプロバイダ２は、ディジタル化されたコンテンツを有し、自己のコンテンツであることを証明するために電子透かし（ウォータマーク（Watermark））をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、コンテンツの取扱方針を生成し、署名データを付加してサービスプロバイダ３へ送信する。

【００１７】

サービスプロバイダ３は、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク４を介して、コンテンツプロバイダ２から供給されたコンテンツに価格情報を追加し、署名データを付加して、ユーザホームネットワーク５に送信する。

【００１８】

ユーザホームネットワーク５は、サービスプロバイダ３から価格情報を付して送付されたコンテンツを入手し、コンテンツ利用権を購入し、購入処理を実行する。購入した利用権は、例えば再生利用権であったり、コピーする権利であったりする。そして、購入処理により生成された課金情報は、ユーザの保持する機器の、暗号処理部内の耐タンパメモリに保存され、ユーザホームネットワーク５が配送鍵K_dを電子配信サービスセンタ１から入手する際に、電子配信サービスセンタ１に送信される。

【００１９】

図２は、電子配信サービスセンタ１の機能の構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３にサービスプロバイダ３の公開鍵証明書及び利益分配の情報を供給すると共に、必要に応じてコンテンツに付される情報（価格情報）を受信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に個別鍵K_i、配送鍵K_dで暗号化した個別鍵K_iおよびコンテンツプロバイダ２の公開鍵証明書を送信すると共に、利益分配の情報を供給し、必要に応じてコンテンツに付される情報（取扱方針）を受信する。著作権管理部１３は、ユーザホームネットワーク５のコンテンツ利用の実績を示す情報を、著作権を管理する団体、例えば、ＪＡＳＲＡＣ（Japanese Society for Rights of Authors, Composers and Publishers：日本音楽著作権協会）に送信する。鍵サーバ１４は、システム全てに使用する鍵の生成、保持、管理を行っており、例えば、コンテンツプロバイダ毎に異なる個別鍵K_iが生成されるとともに、配送鍵K_dで暗号化された個別鍵K_iも併せて生成され、これらはコンテンツプロバイダ管理部１２を介してコンテンツプロバイダ２に供給され、さらに配送鍵K_dで暗号化された個別鍵K_iも必要に応じて認証局２２に供給され、配送鍵

K_d はユーザ管理部１８を介してユーザホームネットワーク５に供給される。また、電子配信サービスセンタ１の公開鍵・秘密鍵、ユーザの保持する機器に固有の公開鍵・秘密鍵も全て生成、管理され、公開鍵は認証局２２に送信され、公開鍵証明書作成に利用される。また、後述する暗号処理部９２に固有の機器別ＩＤに応じた保存鍵K_{save}を生成、保持する場合もある。

【００２０】

電子配信サービスセンタ１からコンテンツプロバイダ２およびユーザホームネットワーク５を構成するホームサーバ５１（後述する）への、鍵の定期的な送信の例について、図３乃至図６を参照に説明する。図３は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成するホームサーバ５１がコンテンツの利用を開始する、２０００年１月における、電子配信サービスセンタ１が有する配送鍵K_d、個別鍵K_i、コンテンツプロバイダ２が有する個別鍵K_i、およびホームサーバ５１が有する配送鍵K_dを示す図である。なお、以下省略するが、コンテンツプロバイダ２は、個別鍵K_iに対応する、配送鍵K_dで暗号化された個別鍵K_iも保持しているものとする。

【００２１】

図３の例において、配送鍵K_d、個別鍵K_iは、暦の月の初日から月の末日まで、使用可能であり、例えば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送鍵K_d、”ｚｚｚｚｚｚｚｚ”の値を有するバージョン１である個別鍵K_iは、２０００年１月１日から２０００年１月３１日まで使用可能（すなわち、２０００年１月１日から２０００年１月３１日の期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵K_{co}は、バージョン１である個別鍵K_iで暗号化され、バージョン１である個別鍵K_iは、バージョン１である配送鍵K_dで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送鍵K_d、”ｙｙｙｙｙｙｙｙ”の値を有するバージョン２である個別鍵K_iは、２０００年２月１日から２０００年２月２９日まで使用可能（すなわち、その期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵K_{co}は、バージョン

２である個別鍵K_iで暗号化され、バージョン２である個別鍵K_iは、バージョン２である配送鍵K_dで暗号化されている）である。同様に、バージョン３である配送鍵K_d、個別鍵K_iは２０００年３月中に使用可能であり、バージョン４である配送鍵K_d、個別鍵K_iは２０００年４月中に使用可能であり、バージョン５である配送鍵K_d、個別鍵K_iは２０００年５月中に使用可能であり、バージョン６である配送鍵K_d、個別鍵K_iは２０００年６月中に使用可能である。

【００２２】

コンテンツプロバイダ２がコンテンツの提供を開始するのに先立ち、電子配信サービスセンタ１は、コンテンツプロバイダ２に、２０００年１月から６月まで利用可能な、バージョン１乃至バージョン６の６つの個別鍵K_iと、それぞれを同一バージョンの配送鍵K_dで暗号化したものを送信し、コンテンツプロバイダ２は、６つの個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iを受信し、記憶する。６月分の個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iを記憶するのは、コンテンツプロバイダ２は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵K_{co}の暗号化などの準備に、所定の期間が必要だからである。

【００２３】

また、ホームサーバ５１がコンテンツの利用を開始するのに先立ち、電子配信サービスセンタ１は、ホームサーバ５１に２０００年１月から２０００年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送鍵K_dを送信し、ホームサーバ５１は、３つの配送鍵K_dを受信し、記憶する。３月分の配送鍵K_dを記憶するのは、ホームサーバ５１が、回線の混雑等を原因として、電子配信サービスセンタ１に接続できないなどのトラブルにより、コンテンツの購入が可能な契約期間にもかかわらずコンテンツが購入できない等の事態を避けるためであり、また、電子配信サービスセンタ１への接続の頻度を低くしたり、個々の機器の電子配信サービスセンタ１への同時アクセスを押さえ、電子配信サービスセンタ１の負荷を低減するためである。

【００２４】

２０００年１月１日から２０００年１月３１日の期間には、バージョン１であ

る配送鍵K_dおよび個別鍵K_iが、電子配信サービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するホームサーバ５１で利用される。

【００２５】

２０００年２月１における、電子配信サービスセンタ１の配送鍵K_dおよび個別鍵K_iのコンテンツプロバイダ２、およびホームサーバ５１への送信を図４で説明する。電子配信サービスセンタ１は、コンテンツプロバイダ２に、２０００年２月から２０００年７月まで利用可能な、バージョン２乃至バージョン７の６つの個別鍵K_iと、それぞれを同一バージョンの配送鍵K_dで暗号化したものを送信し、コンテンツプロバイダ２は、６つの個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iを受信し、受信前に記憶していた個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iに上書きし、新たな個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iを記憶する。電子配信サービスセンタ１は、ホームサーバ５１に２０００年２月から２０００年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送鍵K_dを送信し、ホームサーバ５１は、３つの配送鍵K_dを受信し、受信前に記憶していた配送鍵K_dに上書きし、新たな配送鍵K_dを記憶する。電子配信サービスセンタ１は、バージョン１～７である配送鍵K_dおよび個別鍵K_iをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵K_dを利用できるようにするためである。

【００２６】

２０００年２月１日から２０００年２月２９日の期間には、バージョン２である配送鍵K_dおよび個別鍵K_iが、電子配信サービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するホームサーバ５１で利用される。

【００２７】

２０００年３月１における、電子配信サービスセンタ１の配送鍵K_dおよび個別鍵K_iのコンテンツプロバイダ２、およびホームサーバ５１への送信を図５で説明する。電子配信サービスセンタ１は、コンテンツプロバイダ２に、２０００

年３月から２０００年８月まで利用可能な、バージョン３乃至バージョン８の６つの個別鍵K_iと、それぞれを同一バージョンの配送鍵K_dで暗号化したものを送信し、コンテンツプロバイダ２は、６つの個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iを受信し、受信前に記憶していた個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iに上書きし、新たな個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iを記憶する。電子配信サービスセンタ１は、ホームサーバ５１に２０００年３月から２０００年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送鍵K_dを送信し、ホームサーバ５１は、３つの配送鍵K_dを受信し、受信前に記憶していた配送鍵K_dに上書きし、新たな配送鍵K_dを記憶する。電子配信サービスセンタ１は、バージョン１～８である配送鍵K_dおよび個別鍵K_iをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵K_dを利用できるようにするためである。

【００２８】

２０００年３月１日から２０００年３月３１日の期間には、バージョン３である配送鍵K_dおよび個別鍵K_iが、電子配信サービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するホームサーバ５１で利用される。

【００２９】

２０００年４月１における、電子配信サービスセンタ１の配送鍵K_dおよび個別鍵K_iのコンテンツプロバイダ２、およびホームサーバ５１への送信を図６で説明する。電子配信サービスセンタ１は、コンテンツプロバイダ２に、２０００年４月から２０００年９月まで利用可能な、バージョン４乃至バージョン９の６つの個別鍵K_iと、それぞれを同一バージョンの配送鍵K_dで暗号化したものを送信し、コンテンツプロバイダ２は、６つの個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iを受信し、受信前に記憶していた個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iに上書きし、新たな個別鍵K_iおよび配送鍵K_dで暗号化された個別鍵K_iを記憶する。電子配信サービスセンタ１は、ホームサーバ５１に２０００年４月から２０００年６月まで利用可能な、バージョン４乃至

バージョン６である３つの配送鍵K_dを送信し、ホームサーバ５１は、３つの配送鍵K_dを受信し、受信前に記憶していた配送鍵K_dに上書きし、新たな配送鍵K_dを記憶する。電子配信サービスセンタ１は、バージョン１～９である配送鍵K_dおよび個別鍵K_iをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵K_dを利用できるようにするためである。

【００３０】

２０００年４月１日から２０００年４月３０日の期間には、バージョン４である配送鍵K_dおよび個別鍵K_iが、電子配信サービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するホームサーバ５１で利用される。

【００３１】

このように、あらかじめ先の月の配送鍵K_dおよび個別鍵K_iを配布しておくことで、仮にユーザが１、２ヶ月全くセンタにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センタにアクセスすることにより鍵を受信することができる。

【００３２】

電子配信サービスセンタ１の経歴データ管理部１５（図２）は、ユーザ管理部１８が集めたコンテンツの利用の実績を示す情報である課金情報、必要に応じてそのコンテンツに対応する価格情報（サービスプロバイダ３から送られてくるものと、ユーザが課金情報に付加して送ってくるものの、どちらか一方又は両方）、および必要に応じてそのコンテンツに対応する取扱方針（コンテンツプロバイダ２から送られてくるものと、ユーザが課金情報に付加して送ってくるものの、どちらか一方又は両方）を保持・管理し、サービスプロバイダ管理部１１又はコンテンツプロバイダ管理部１２等が課金情報や利用履歴等を利用する際にデータを出力する。なお、価格情報及び取扱方針は、課金情報に必要なデータが書き込まれている場合サービスプロバイダ３やコンテンツプロバイダ２から送られてこない場合がある。利益分配部１６は、経歴データ管理部１５から供給された、課金情報、必要に応じて価格情報、および取扱方針に基づき、電子配信サービスセ

ンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３の利益を算出する。これらの情報は、出納部２０へ供給され、出納部２０を介して利益分配を行う場合もあるが、利益分配を行なわず、これらの情報のみをサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、著作権管理部１３に送信し、売上そのものはサービスプロバイダに入金させ、サービスプロバイダ３が各受益者に利益を分配する場合がある。相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の所定の機器と後述する相互認証を実行する。

【００３３】

ユーザ管理部１８は、ユーザ登録データベースを有し、ユーザホームネットワーク５の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒否する等の登録情報を作成する。ユーザホームネットワーク５が電子配信サービスセンタ１と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部１８は、登録情報に決済をする機器を規定し、決済ＩＤを登録し、更に、コンテンツの購入処理動作を規定したり、ユーザホームネットワークを構成する機器の範囲を規定したり、取引停止等の情報を規定し、ユーザホームネットワーク５の所定の機器（決済可能機器）に送信する。

【００３４】

図７に示すユーザ登録データベースの例は、ユーザホームネットワーク５内で構築されたネットワークグループ毎の登録状況を示したもので、各グループには、グループのＩＤを示すグループＩＤ、ホームネットワーク５を構成する機器に固有のＩＤ、そのＩＤに対応して（すなわち、そのＩＤを有する機器毎に）、電子配信サービスセンタ１と接続が可能か否か、決済処理可能か否か、コンテンツの購入ができるか否か、決済処理を行うのはどの機器か、コンテンツの購入を依頼する機器はどれか、登録可能か否か、等の情報を記録する。

【００３５】

ユーザ登録データベースに記録されたグループＩＤはユーザホームネットワーク毎に割り振られ、このグループ単位で決済、情報更新が行われる。従って、原

則的にはグループ内の代表機器が電子配信サービスセンタ１と通信、決済処理、情報更新を一括して行い、グループ内の他の機器は電子配信サービスセンタ１とのやりとりを直接は行わない。ユーザ登録データベースに記録されたＩＤは、機器毎に個別に割り振られたＩＤで、機器を識別するのに使用される。

【００３６】

ユーザ登録データベースに記録された電子配信サービスセンタ１と接続が可能か否かの情報は、その機器が、電子配信サービスセンタ１と物理的に接続が可能であるか否かを示し、接続できると記録された機器でも、決済処理可能であるとされた機器以外は、原則的に電子配信サービスセンタ１に接続されることがない（ただし、グループ内の代表機器が何らかの原因で決済処理動作しなくなった場合、代理で一時的に電子配信サービスセンタ１に接続されることはある）。また、接続ができないと記録された機器は、ユーザホームネットワーク５の決済処理可能な機器を介して、電子配信サービスセンタ１に、課金情報等を出力する。

【００３７】

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク５が、コンテンツの利用権の購入などが可能な複数の機器で構成されているとき、その中の決済処理が可能である１台の機器は、電子配信サービスセンタ１に、ユーザホームネットワーク５の電子配信サービスセンタ１に登録されている全ての機器の、課金情報、必要に応じて価格情報、および取扱方針を送信し、決済処理の完了に応じて電子配信サービスセンタ１から配送鍵K_d、登録情報を受信する。こうすることで、機器毎に処理を行うのに比べ、電子配信サービスセンタ１の処理が軽減される。

【００３８】

ユーザ登録データベースに記録された購入処理が可能か否かの情報は、その機器が、コンテンツの利用権の購入ができるか否かを表す。購入不可の機器においては、他の購入可の機器から利用権の代理購入（別の機器で権利を購入し、その権利を全て譲り受けるものを言う。供給側には全く権利は残らない）、再配布（既に購入したコンテンツの利用権を、同一利用権内容または異なる利用権内容でもう一度購入し、別機器に供給する方式を言う。このとき、供給側には全く権利

は残らない。再配布は、割引を行うことを主たる目的とする。割引の特典を受けられるのは、同一決済ＩＤを使用しているグループであることが条件である。なぜなら、同一決済ＩＤに属するグループ内の処理においては、電子配信サービスセンタ１の処理負担が軽減され、従って、その代償として割引が受けられるからである）または管理移動（コンテンツ再生権、特に無期限再生権の移動ができるが、再生権送信器においては再生権受信器がどの機器であるか管理され、再生権の返還がない場合、再度管理移動ができず、再生権受信器においては、再生権送信器がどの機器であるかが管理され、再度管理移動が全くできず、唯一、再生権を与えてくれた再生権送信器に再生権を返還することのみできる）を行ってもらってコンテンツ利用権を取得する。

【００３９】

ここで、コンテンツの利用方法／利用権及び購入方法について簡単に説明する。コンテンツの利用方法としては、コンテンツの利用権を自己で管理保持しているものが利用する場合と、他機器の保持する利用権を行使して自己の機器において利用する、２つのものがある。コンテンツの利用権としては、無制限再生権（コンテンツの再生期間及び回数に制限がないもの、なお、音楽コンテンツの場合は再生であるが、ゲームプログラム等では実行になる）、時間制限付き再生権（コンテンツの再生できる期間が限られているもの）、回数制限付き再生権（コンテンツの再生できる回数が限られているもの）、無制限複製権（コンテンツの複製期間及び回数に制限がないもの）、回数制限付き複製権（コンテンツの複製に回数制限があるもの）（複製権には、コピー管理情報なし複製権、コピー管理情報付き複製権（SCMS）等、その他専用メディア向け複製権等がある）（また時間制限付き複製権もある場合がある）、管理移動権がある。そして、利用権の購入方法としては、これらの利用権を直接購入する通常の購入に加え、既に購入した利用権の内容を別の内容に変更する利用権内容変更、他の機器で既に購入した権利に基づき利用権を別途購入する再配布、他の機器で利用権の購入を代理で行ってもらう代理購入、複数のコンテンツ利用権を一括して購入管理するアルバム購入等がある。

【００４０】

ユーザ登録データベースに記録された代理決済者に記された情報は、コンテンツの利用権を購入した際に生成した課金情報を、代理で電子配信サービスセンタ１に送信してもらう機器のＩＤを示す。

【００４１】

ユーザ登録データベースに記録された代理購入者に記された情報は、コンテンツの利用権の購入ができない機器に対し、代理で利用権の購入を行ってくれる機器のＩＤを示す。ただし、購入処理可能なグループ内機器全てが代理購入者ということにしてした場合には、特に記録しておく必要はない。

【００４２】

ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）、またはクレジットカード会社などから供給される料金の未払い、不正処理等の情報を基に、更新される。登録が不可と記録されたＩＤを有する機器の登録の要求に対して、ユーザ管理部１８は、その登録を拒否し、登録を拒否された機器は、以降、このシステムのコンテンツの購入ができないだけでなく、ユーザホームネットワーク５内の他機器とのデータ送受信もできなくなる。また場合によっては購入済のコンテンツの利用も制限される場合がある（ただし、電子配信サービスセンタ１等に機器を持ち込み、検査等を済ませた後再登録されることはある）。また、「登録可」、「登録不可」だけでなく、「決済未処理」、「一時停止」等の状態もあり得る。

【００４３】

また、ユーザ管理部１８は、ユーザホームネットワーク５の機器から課金情報、登録情報、必要に応じて価格情報や取扱方針が供給され、課金情報、価格情報、および取扱方針を経歴データ管理部１５に出力し、ユーザホームネットワーク５の機器に、配送鍵K_d、登録情報を供給する。供給されるタイミングについては後述する。

【００４４】

ここで、図８を用いて登録情報を説明する。図８の登録情報はユーザ登録データベースの情報に加え、決済ＩＤおよび署名が付加されており、同一決済グルー

プの情報のみが含まれている。決済ＩＤとは、決済を行う際に課金請求部１９および出納部２０が使用するユーザの、ユーザ情報データベース（例えば銀行口座番号やクレジットカード番号）内のＩＤを示している。署名の生成については、後述する。

【００４５】

再び図２にもどり、課金請求部１９は、経歴データ管理部１５から供給された、課金情報、必要に応じて価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部２０に供給する。また、必要に応じてユーザ管理部１８を介してユーザに決済情報を提供する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決済処理を実行する。なお、出納部２０は、サービスプロバイダ３へ売上のすべてを送金させ、利益分配部１６を介して送信された分配金情報をもとに、サービスプロバイダ３が利益分配をする場合がある。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針を、コンテンツプロバイダ２から供給された取扱方針と、サービスプロバイダ３から供給された価格情報とからその正当性を監査する。

【００４６】

また、監査部２１の処理としては、ユーザホームネットワーク５から入金された金額と、利益分配した合計金額又はサービスプロバイダ３へ送った金額との整合性を監査する処理や、ユーザホームネットワーク５の機器から供給された課金情報内のデータに例えば存在し得ないコンテンツプロバイダＩＤ、サービスプロバイダＩＤや考えられない取り分、価格等が含まれているか否かを監査する処理がある。

【００４７】

認証局２２は、鍵サーバ１４から供給された公開鍵の証明書を生成し、コンテンツプロバイダ２、サービスプロバイダ３へ供給し、ユーザ機器製造時にホームサーバ５１の大容量記憶部６８（後述する）や、据置機器５２の小容量記憶部７５（後述する）に保存される公開鍵証明書も生成する。コンテンツプロバイダ２

がコンテンツのオーサリングを行わない場合、これを代替えする方法として、コンテンツを保持するコンテンツサーバ２３、コンテンツオーサリング２４がある。

【００４８】

図９は、コンテンツプロバイダ２の機能の構成を示すブロック図である。コンテンツサーバ３１は、ユーザに供給するコンテンツを記憶し、電子透かし（ウォータマーク）付加部３２に供給する。電子透かし付加部３２は、コンテンツサーバ３１から供給されたコンテンツに自分の所有物であることを示すコンテンツプロバイダＩＤを電子透かしの形で挿入し、圧縮部３３に供給する。圧縮部３３は、電子透かし付加部３２から供給されたコンテンツを、ＡＴＲＡＣ（Adaptive Transform Acoustic Coding）（商標）等の方式で圧縮し、コンテンツ暗号部３４に供給する。因に、圧縮方式としてはＡＴＲＡＣに代えてＭＰ３やＡＡＣ等の方式を用いることができる。コンテンツ暗号部３４は、圧縮部３３で圧縮されたコンテンツを、コンテンツ鍵生成部３５から供給された鍵（以下、この鍵をコンテンツ鍵K_{co}と称する）を用いて、ＤＥＳ（Data Encryption Standard）などの共通鍵暗号方式で暗号化し、その結果を署名生成部３８に出力する。

【００４９】

コンテンツ鍵生成部３５は、コンテンツ鍵K_{co}となる所定のビット数の乱数を生成し、この中で弱鍵（例えば、K_{co}＝１Ｅ１Ｅ１Ｅ１Ｅ０Ｅ０Ｅ０Ｅ０Ｅや１ＥＥ０１ＥＥ００ＥＦ００ＥＦ０など）と呼ばれる暗号化に不適なビット列を除いたものをコンテンツ暗号部３４、コンテンツ鍵暗号部３６に供給する。そのような不適なビット列がない暗号アルゴリズムを使用するときは、不適なビット列を除く処理は不要である。コンテンツ鍵暗号部３６は、コンテンツ鍵K_{co}を電子配信サービスセンタ１から供給された個別鍵K_iを使用して、ＤＥＳなどの共通鍵暗号方式で暗号化し、その結果を署名生成部３８に出力する。因に、暗号化方式としては、ＤＥＳに限らず、例えばＲＳＡ（Rivest,Shamir,Adleman）等の公開鍵暗号方式を用いるようにしても良い。

【００５０】

ＤＥＳは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして

処理する暗号方式である。ＤＥＳの処理は、平文を撹拌し、暗号文に変換する部分（データ撹拌部）と、データ撹拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。ＤＥＳの全てのアルゴリズムは公開されているので、ここでは、データ撹拌部の基本的な処理を簡単に説明する。

【００５１】

まず、平文６４ビットは、上位３２ビットのＨ０、および下位３２ビットのＬ０に分割される。鍵処理部から供給された４８ビットの拡大鍵Ｋ１、および下位３２ビットのＬ０を入力として、下位３２ビットのＬ０を撹拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成される。次に、上位３２ビットのＨ０と、Ｆ関数の出力が排他的論理和され、その結果はＬ１とされる。Ｌ０は、Ｈ１とされる。

【００５２】

上位３２ビットのＨ０および下位３２ビットのＬ０を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのＨ１６および下位３２ビットのＬ１６が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【００５３】

なお、本実施の形態では共通鍵暗号としてＤＥＳを示したが、ＮＴＴ（商標）が提案するＦＥＡＬ（Fast Encryption Algorithm ）、ＩＤＥＡ（International Data Encryption Algorithm ）、Ｅ２や、米国次期暗号標準であるＡＥＳ（Advanced Encryption Standard）など、いずれでもよい。

【００５４】

取扱方針生成部３７は、コンテンツの取扱方針を生成し、暗号化されるコンテンツに対応して、取扱方針を署名生成部３８に出力する。なお、取扱方針生成部３７は、生成した取扱方針を図示せぬ通信手段を介して電子配信サービスセンタ１に供給する場合があり、そのデータは保持・管理されている。署名生成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、暗号化された個別鍵K_i、取扱方針に電子署名を付加し、コンテンツプロバイダ２の証明書Ｃｃ

ｐと共にサービスプロバイダ３に送信する（以降、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、暗号化された個別鍵K_i、取扱方針のそれぞれにコンテンツプロバイダ３の秘密鍵を使用して電子署名を付加したものを、コンテンツプロバイダセキュアコンテナと称する）。なお、個々のデータに署名を別々に付加するのではなく、データ全体に対して１つの署名を付けるようにしてもよい。

【００５５】

相互認証部３９は、電子配信サービスセンタ１と相互認証し、また、必要に応じてサービスプロバイダ３へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証する。メモリ４０Ａは、コンテンツプロバイダ２が秘密裏に保持しなくてはならない個別鍵K_iを保持するため、第３者に容易にデータを読み出されない耐タンパメモリが望ましいが、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。また、メモリ４０Ｂは、配送鍵K_dで暗号化された個別鍵K_i、コンテンツプロバイダ２の公開鍵証明書が保存されるだけであるため、通常の記憶装置等何でもよい（公開情報であるため、秘密にする必要がない）。なお、メモリ４０Ａ、４０Ｂを一つにしてもかまわない。

【００５６】

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵を使用して作成される。

【００５７】

ハッシュ関数および署名ついて説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ（Message Dige

st）４、ＭＤ５、ＳＨＡ（Secure Hash Algorithm）－１などが用いられる。

【００５８】

データと署名を送信する送信装置（コンテンツプロバイダ２）の署名生成部３８は、例えば、公開鍵暗号方式である楕円曲線暗号を用いて署名を生成する。この処理を、図１０を用いて説明する（EC-DSA（Elliptic Curve Digital Signature Algorithm）、IEEE P1363/D3）。ステップＳ１で、Ｍをメッセージ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2 = x^3 + ax + b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、K_sを秘密鍵（$0 < K_s < r$）とする。ステップＳ２で乱数ｕを$0 < u < r$になるように乱数発生ユニットで生成する。ステップＳ３でベースポイントをｕ倍した座標を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

【００５９】

$P = (X_0, Y_0)$、$Q = (X_1, Y_1)$、$R = (X_2, Y_2) = P + Q$とし、

$P \neq Q$の時、

$$X_2 = \lambda^2 - X_0 - X_1$$
$$Y_2 = \lambda (X_0 - X_2) - Y_0$$
$$\lambda = (Y_1 - Y_0) / (X_1 - X_0)$$

$P = Q$の時、

$$X_2 = \lambda^2 - 2X_0$$
$$Y_2 = \lambda (X_0 - X_2) - Y_0$$
$$\lambda = (3X_0^2 + a) / 2Y_0$$

となり、これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。Ｇ、２Ｇ、４Ｇ・・を計算し、ｕを２進数展開して１が立っているところに対応する$(2^i) \times G$を加算する（ｉはｕのＬＳＢから数えた時のビット位置））。ステップＳ４で$c = X_v \mod r$を計算し、ステップＳ５でこの値が０になるかどうか判定し、０でなければステップＳ６へと進み、メッセージＭのハッシュ値を計算し、ｆ＝ＳＨＡ－１（Ｍ）とする。次に、ステップＳ７において、$d = [(f + cK_s) / u] \mod r$を計算し、ステップＳ８でｄが０であるかどうか判定する。ｄが０出なければ、ｃ

およびｄを署名データとする。仮に、ｒを１６０ビット長の長さであると仮定すると、署名データは３２０ビット長となる。

【００６０】

ステップＳ５において、ｃが０であった場合、ステップＳ２に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ２に戻って乱数を生成し直す。

【００６１】

署名とデータを受信した受信装置（ユーザホームネットワーク５）は、例えば、公開鍵暗号方式である楕円曲線暗号を用いて署名を検証する。この処理を、図１１を用いて説明する。（受信装置は）ステップＳ１０で、Ｍをメッセージ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2 = x^3 + ax + b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびK_s Ｇを公開鍵（$0 < K_s < r$）とする。ステップＳ１１で署名データｃおよびｄが$0 < c$、$d < r$を満たすか検査する。これを満たしていた場合、ステップＳ１２で、メッセージＭのハッシュ値を計算し、ｆ＝ＳＨＡ－１（Ｍ）とする。次に、ステップＳ１３でｈ＝１／ｄ ｍｏｄ ｒ を計算し、ステップＳ１４で$h_1 = fh$、$h_2 = ch \mod r$ を計算する。ステップＳ１５において、既に計算したh_1 およびh_2 を用い、$P = (X_p, Y_p) = h_1 G + h_2 K_s G$を計算する。署名検証者は、公開鍵ＧおよびＫｓＧを知っているので、ステップＳ３と同様にこの計算ができる。そして、ステップＳ１６でＰが無限遠点かどうか判定し、無限遠点でなければステップＳ１７に進む（実際には、無限遠点の判定はステップＳ１５でできてしまう。つまり、Ｐ＝（Ｘ、Ｙ）、Ｑ＝（Ｘ、－Ｙ）の加算を行うと、前述のλが計算できず、Ｒが無限遠点であることが判明している。ステップＳ１７で$X_p \mod r$を計算し、署名データｃと比較する。この値が一致していた場合、ステップＳ１８に進み、署名が正しいと判定する。

【００６２】

署名が正しいと判定された場合、受信データは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信装置から送信されたデータであることがわかる。

【００６３】

ステップＳ１１において、署名データｃおよびｄが０＜ｃ、ｄ＜ｒを満たさなかった場合、ステップＳ１９に進む。また、ステップＳ１６において、Ｐが無限遠点であった場合もステップＳ１９に進む。さらにまた、ステップＳ１７において、X_p　ｍｏｄ　ｒの値が、署名データｃと一致していなかった場合にもステップＳ１９に進む。ステップＳ１９において、署名が正しくないと判定する。

【００６４】

署名が正しくないと判定された場合、受信データは改竄されているか、公開鍵に対応した秘密鍵を保持する送信装置から送信されたデータではないことがわかる。

【００６５】

なお、本実施の形態では、ハッシュ関数としてＳＨＡ－１を使用したが、ＭＤ４、ＭＤ５などいずれの関数を使用してもよい。また、署名の生成および検証はＲＳＡ暗号を用いて行ってもよい（ＡＮＳＩ　Ｘ９．３１－１）。

【００６６】

次に公開鍵暗号方式の暗号化・復号化について説明する。暗号化および復号化で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対して、公開鍵暗号方式は、暗号化に使用する鍵と復号化に使用する鍵が異なる。公開鍵暗号方式を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開してもよい鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【００６７】

公開鍵暗号方式の中で代表的な楕円曲線暗号化方法を説明する。図１２において、ステップＳ２０で、M_x、M_yをメッセージ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2 = x^3 + ax + b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびK_s　Ｇを公開鍵（$0 < K_s < r$）とする。ステップＳ２１で乱数ｕを$0 < u < r$になるように生成する。ステップＳ２２で公開鍵K_s　Ｇをｕ倍した座標Ｖを計算する。なお、楕円曲線上のスカラー倍は署名生成のところで説明した方法と同一のため、ここでは説明を省略する。ステップＳ２３で、ＶのＸ座標をM_x倍してｐで剰余を求めX_0とする。ステップＳ２４でＶのＹ

座標をM_y倍してｐで剰余を求めY_0とする。なお、メッセージの長さがｐのビット数より少ない場合、M_yは乱数を使い、復号部ではM_yを破棄するようにする。ステップＳ２５において、ｕＧを計算し、ステップＳ２６で暗号文ｕＧ、（X_0、Y_0）を得る。

【００６８】

ここで公開鍵暗号方式の復号化について、図１３を用いて説明する。ステップＳ３０において、ｕＧ、（X_0、Y_0）を暗号文データ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2 = x^3 + ax + b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、K_sを秘密鍵（$0 < K_s < r$）とする。ステップＳ３１において、暗号データｕＧを秘密鍵K_s倍する。ステップＳ３２では、暗号データの内、（X_0、Y_0）のＸ座標を取り出し、$X_1 = X_0 / X_v \mod p$を計算する。ステップＳ３３においては、$Y_1 = Y_0 / Y_v \mod p$を計算する。そして、ステップＳ３４でX_1をM_xとし、Y_1をM_yとしてメッセージを取り出す。この時、M_yをメッセージにしていなかった場合、Y_1は破棄する。

【００６９】

このように公開鍵暗号方式では、秘密鍵をK_s、公開鍵をＧ、K_sＧとすることで、暗号化に使用する鍵と復号化に使用する鍵を、異なる鍵とすることができる。

【００７０】

また、公開鍵暗号方式の他の例としてはＲＳＡ暗号（Rivest、Shamir、Adleman）が知られている。

【００７１】

図１４は、サービスプロバイダ３の機能の構成を示すブロック図である。コンテンツサーバ４１は、コンテンツプロバイダ２から供給された、コンテンツプロバイダ２の公開鍵証明書および暗号化されているコンテンツを記憶している。コンテンツプロバイダ２の公開鍵証明書は、証明書検査部４２で、証明書内の署名が認証局２２の公開鍵で検証され、検証に成功した場合、コンテンツプロバイダ２の公開鍵を署名検証部４３に供給する。署名検証部４３においては、コンテンツサーバ４１に記憶されている取扱方針に対するコンテンツプロバイダ２の署名

を、先ほど検証したコンテンツプロバイダ２の公開鍵を用いて検証し、検証に成功した場合、取扱方針を値付け部４４に供給する。値付け部４４においては、取扱方針から価格情報を作成し、署名生成部４５に供給する。署名生成部４５においては、図示せぬ耐タンパメモリ（コンテンツプロバイダ２内の４０Ａと同様）に保持されたサービスプロバイダ３の秘密鍵を用い、価格情報に対する署名を生成する（以降、コンテンツプロバイダセキュアコンテナおよび価格情報にサービスプロバイダ３の秘密鍵を用いて電子署名を付加したものを、サービスプロバイダセキュアコンテナと称する）。なお、価格情報に署名を付加するのではなく、コンテンツプロバイダセキュアコンテナと価格情報全体に対して１つの署名を生成するようにしてもよい。そして、サービスプロバイダセキュアコンテナ、コンテンツプロバイダ２の公開鍵証明書、サービスプロバイダ３の公開鍵証明書を、ネットワーク４（図１）を介してユーザホームネットワーク５へ供給する。相互認証部４６は、電子配信サービスセンタ１と相互認証し、また、必要に応じてコンテンツプロバイダ、およびインターネット、ケーブル通信等を介し、可能であればユーザホームネットワーク５と相互認証する。

【００７２】

図１５は、ユーザホームネットワーク５の構成を示すブロック図である。ホームサーバ５１は、ネットワーク４を介して、サービスプロバイダ３からコンテンツを含んだセキュアコンテナを受信し、コンテンツの利用権を購入し、その権利を行使してコンテンツの復号、伸張、再生、複製を行う。

【００７３】

通信部６１は、ネットワーク４を介してサービスプロバイダ３、または電子配信サービスセンタ１と通信し、所定の情報を受信し、または送信する。上位コントローラ６２は、入力手段６３からの信号を受信し、所定のメッセージ等を表示手段６４に表示し、暗号処理部６５を利用してコンテンツの利用権購入処理等を行い、伸張部６６に大容量記憶部６８から読み出した暗号化されたコンテンツを供給し、大容量記憶部６８に暗号化されたコンテンツ等を記憶する。入力手段６３は、リモートコントローラからの信号や入力ボタンからの入力データを上位コントローラ６２に送信する。表示手段６４は、液晶表示器のような表示デバイス

で構成され、ユーザに指示を出したり、情報を表示したりする。入力手段６３および表示手段６４は、必要に応じてタッチパネル式液晶表示器などになり、一つにまとめられる場合がある。暗号処理部６５は、サービスプロバイダ３、または電子配信サービスセンタ１若しくはその他の機器の暗号処理部と相互認証し、コンテンツ利用権を購入すると共に、所定のデータの暗号化／復号化を行い、コンテンツ鍵K_{co}および使用許諾条件情報を保持する外部メモリを管理し、さらに配送鍵K_d、課金情報等を記憶する。伸張部６６は、暗号処理部６５と相互認証してコンテンツ鍵K_{co}を受信し、このコンテンツ鍵K_{co}を用いて上位コントローラ６２から供給された暗号化されたコンテンツを復号化し、ＡＴＲＡＣ等の所定の方式で伸張し、さらに所定の電子透かしをコンテンツに挿入する。外部メモリ６７は、フラッシュメモリ等の不揮発メモリやバックアップ電源付き揮発性メモリで構成され、保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}および使用許諾条件情報を保存する。大容量記憶部６８はＨＤＤや光ディスク等の記憶デバイスで、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナ（暗号化されたコンテンツ、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}、配送鍵K_dで暗号化された個別鍵K_i、取扱方針、価格情報及びそれらの署名）、公開鍵証明書、登録情報等が保存されている。

【００７４】

電子配信サービスセンタ１と相互認証し、コンテンツ利用権を購入すると共に課金情報を生成し、所定のデータの復号化／暗号化を行い、コンテンツ鍵K_{co}および使用許諾条件情報を保持する外部メモリを管理し、さらに配送鍵K_d、課金情報等を記憶する暗号処理部６５は、制御部９１、記憶モジュール９２、登録情報検査モジュール９３、購入処理モジュール９４、相互認証モジュール９５、暗号／復号化モジュール９６、および外部メモリ制御部９７から構成される。この暗号処理部６５は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパ性）を有する。

【００７５】

制御部９１は、上位コントローラ６２からのコマンドに応じて各モジュールを制御すると共に、各モジュールからの結果を上位コントローラ６２に返送する。記憶モジュール９２は、購入処理モジュール９４から供給された課金情報、および配送鍵K_d等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送鍵K_d等のデータを供給する。登録情報検査モジュール９３は、上位コントローラ６２から供給された登録情報を検査し、ユーザホームネットワーク５内の他の機器と相互認証するか否か、課金情報の授受をすべきか否か、コンテンツの再配布等をすべきか否かの判断を行う。購入処理モジュール９４は、サービスプロバイダ３から受信したセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、既に保持している使用許諾条件情報）から、新たに使用許諾条件情報を生成して外部メモリ制御部９７又は制御部９１に出力し、課金情報を生成して記憶モジュール９２に出力する。相互認証モジュール９５は、電子配信サービスセンタ１、ホームネットワーク５内の他の機器の暗号処理部および伸張部６６との相互認証を実行し、必要に応じて、一時鍵K_{temp}（セッション鍵）を生成し、暗号／復号化モジュール９６に供給する。

【００７６】

復号／暗号化モジュール９６は、復号化ユニット１１１、暗号化ユニット１１２、乱数発生ユニット１１３、署名生成ユニット１１４、および署名検証ユニット１１５から構成される。復号化ユニット１１１は、配送鍵K_dで暗号化された個別鍵K_iを復号化したり、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}を復号化したり、一時鍵K_{temp}で暗号化された各種データを復号化したりする。暗号化ユニット１１２は、復号化されたコンテンツ鍵K_{co}を、記憶モジュール９２に保持されている保存鍵K_{save}で暗号化し、制御部９１を介して外部メモリ制御部９７に出力したり、一時鍵K_{temp}で各種データを暗号化したりする。乱数発生ユニット１１３は、所定の桁数の乱数を発生し、相互認証モジュール９５や署名生成ユニット１１４に供給する。署名生成ユニット１１４は、制御部９１から供給されたメッセージのハッシュ値を計算し、乱数発生ユニット１１３から供給された乱数を用いて署名データを生成して制御部９１に出力する。署名検証ユニット１

１５は、制御部から供給されたメッセージおよび署名データから署名が正しいかどうか判定し、その結果を制御部９１に出力する。なお、署名の生成／検証方法については図１０、図１１について上述した場合と同様である。

【００７７】

外部メモリ制御部９７は、外部メモリ６７を制御してデータの読み書きを行い、外部メモリ内のデータが改竄されていないかどうかデータ検証を行う。図１６は、外部メモリ制御部９７の動作を説明するブロック図である。図１６において、記憶モジュール９２には、Ｎ個の改竄防止用ハッシュ値（Integrity Check Value ）が保存されている。外部メモリ６７は、Ｎブロックのデータ領域に分割されており、それぞれのデータ領域にはM組のコンテンツ鍵K_{co}および使用許諾条件情報が書き込めるようになっている。また、外部メモリ６７には、自由に使用できるその他の領域も用意されている。改竄防止用ハッシュ値ＩＣＶは、それに対応する外部メモリ６７内の全データに対するハッシュ値になっている。外部メモリの読み出し手順および書き込み手順については、フローチャートを用いて後述する。

【００７８】

コンテンツを復号化し、伸張し、所定の電子透かしを付加する伸張部６６（図１５）は、相互認証モジュール１０１、鍵復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、電子透かし付加モジュール１０５、および記憶モジュール１０６から構成される。相互認証モジュール１０１は、暗号処理部６５と相互認証し、一時鍵K_{temp}を鍵復号モジュール１０２に出力する。鍵復号モジュール１０２は、外部メモリ６７から読み出され一時鍵K_{temp}で暗号化されているコンテンツ鍵K_{co}を一時鍵K_{temp}で復号化し、復号モジュール１０３に出力する。復号モジュール１０３は、大容量記憶部６８に記録されたコンテンツをコンテンツ鍵K_{co}で復号化し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号化されたコンテンツを、更にＡＴＲＡＣ等の方式で伸張し、電子透かし付加モジュール１０５に出力する。電子透かし付加モジュール１０５は、購入処理を行った暗号処理部の個別ＩＤを電子透かし技術を用いてコンテンツに挿入し、他の機器や図示せぬスピーカに出力し、音楽を再生する。

【００７９】

記憶モジュール１０６には、暗号処理部６５との相互認証に必要な鍵データが保存されている。なお、伸張部６６は、耐タンパ性を備えていることが望ましい。

【００８０】

外部メモリ６７は、購入処理モジュール９４で権利購入した際に生成した使用許諾条件情報や保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}を記憶している。大容量記憶部６８は、サービスプロバイダ３から供給されたセキュアコンテナや公開鍵証明書、登録情報等を記録する。

【００８１】

装着された光ディスク、半導体メモリ等の記録メディア８０にサービスプロバイダ３から供給されたコンテンツを記録し、再生する据置機器５２は、通信部７１、上位コントローラ７２、暗号処理部７３、伸張部７４、小容量記憶部７５、記録再生部７６、入力手段７７、表示手段７８、外部メモリ７９、および記録メディア８０から構成される。通信部７１は通信部６１と同じ機能を有し、その説明は省略する。上位コントローラ７２は上位コントローラ６２と同じ機能を有し、その説明は省略する。暗号処理部７３は暗号処理部６５と同じ機能を有し、その説明は省略する。伸張部７４は伸張部６６と同じ機能を有し、その説明は省略する。小容量記憶部７５は大容量記憶部６８と同じ機能を有しているものの、コンテンツそのものは保存されず、公開鍵証明書や登録情報等が記憶されるだけである。記録再生部７６は、光ディスク、半導体メモリ等の記録メディア８０が装着され、その記録メディア８０にコンテンツを記録し、読み出したコンテンツを伸張部に出力する。入力手段７７は入力手段６３と同じ機能を有し、その説明は省略する。表示手段７８は表示手段６４と同じ機能を有し、その説明は省略する。外部メモリ７９は外部メモリ６７と同じ機能を有し、その説明は省略する。記録メディア８０は、例えばＭＤ（Mini Disk ：商標）や、電子配信専用記憶メディア（半導体メモリを用いたMemory Stick：商標）であったりする。

【００８２】

ユーザが携帯し、音楽を再生して楽しむための機器である携帯機器５３は、通

信部８１、上位コントローラ８２、暗号処理部８３、伸張部８４、および外部メモリ８５から構成される。通信部８１は通信部６１と同じ機能を有し、その説明は省略する。上位コントローラ８２は上位コントローラ６２と同じ機能を有し、その説明は省略する。暗号処理部８３は暗号処理部６５と同じ機能を有し、その説明は省略する。伸張部８４は伸張部６６と同じ機能を有し、その説明は省略する。外部メモリ８５は外部メモリ６７と同じ機能を有し、その説明は省略する。ただし、これらのメモリは半導体メモリだけとは限らず、ＨＤＤ、書き換え可能な光ディスク等いずれでもよい。

【００８３】

図１７は、電子配信専用の記録メディアの構成図を示したものである。電子配信されたコンテンツを保存する記録メディア１２０は、通信部１２１、暗号処理部１２２、および外部メモリ１２３から構成される。通信部１２１は、据置機器５２（図１５）の記録再生部７６とデータの送受信を行う。据置機器５２と相互認証し、コンテンツ利用権を譲り受け、所定のデータの復号化／暗号化を行い、コンテンツ鍵K_{co}および使用許諾条件情報等を保持する外部メモリを管理し、さらに保存鍵K_{save}等を記憶する暗号処理部１２２は、その構成は暗号処理部６５と同じ機能を有し、その説明は省略する。外部メモリ１２３は、保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}、コンテンツ鍵K_{co}で暗号化されたコンテンツ、コンテンツの使用条件を定めた使用許諾条件情報、必要に応じて取扱方針、および価格情報を記憶している。

【００８４】

電子配信専用記録メディア１２０は、据置機器５２の時に説明した記録メディアとは使い方が異なっている。通常の記録メディア８０は、ホームサーバ５１の大容量記憶部６８の代用品であるのに対し、電子配信専用メディア１２０は、伸張部を持たない携帯機器に異ならない。従って、コンテンツの再生を行う際には、伸張部７４をもつ据置機器５２のような機器が必要であるが、コンテンツを譲り受けたり、コンテンツを管理したりする機能に関してはホームサーバ５１や携帯機器５３と同様な処理ができる。これらの違いにより、通常の記録メディアに記録されたコンテンツは、記録した機器以外では再生することができないものの

、電子配信専用記録メディア１２０に記録されたコンテンツは、記録した機器以外の機器でも再生することができるようになる。すなわち、通常の記録メディアには、コンテンツ鍵K_{co}で暗号化されたコンテンツがあるだけなので、コンテンツ鍵K_{co}を持つ（記録した）機器以外では再生ができない。一方、電子配信専用記録メディア１２０においては、コンテンツ鍵K_{co}で暗号化されたコンテンツだけでなく、コンテンツ鍵K_{co}も、電子配信専用記録メディア１２０個有の保存鍵K_{save}で暗号化されて保持されているため、他の機器で再生することが可能になる。

【００８５】

つまり暗号処理部１２２の相互認証モジュール１２８と据置機器５２の暗号処理部７３の図示せぬ相互認証モジュール間で相互認証を行った後、専用記録メディア固有の保存鍵K_{save3}でコンテンツ鍵K_{CO}を復号化し、共有した一時鍵K_{temp}でコンテンツ鍵K_{co}を暗号化し、暗号処理部７３へ送信して再生する。

【００８６】

図１８は、各機器内のデータ記憶状況を示すブロック図である。ホームサーバ５１において、暗号処理部６５内の記憶モジュール９２には、機器を特定するための個別ＩＤ（暗号処理部を特定するものと同一）、課金処理する際に使用する決済用ＩＤ（必要に応じて個別ＩＤで代替えできるし、登録情報にあるので不要の場合もある）、機器毎に異なる秘密鍵、保存鍵K_{save}、電子配信サービスセンタ１と相互認証する際に使用する電子配信サービスセンタ１の公開鍵（電子配信サービスセンタ１の公開鍵証明書があれば不要）、公開鍵証明書を検証するための認証局２２の公開鍵、伸張部６６と相互認証する際に使用する共通鍵が記憶されている。これらのデータは、機器製造時に予め記憶されるデータである。これに対し、電子配信サービスセンタ１から定期的に配布される配送鍵K_d、購入処理の際に書き込まれる課金情報、外部メモリ６７内に保持するコンテンツ鍵K_{co}および使用許諾条件情報の改竄チェック用のハッシュ値は、機器を使用し始めてから記憶されるデータであり、これらのデータも記憶モジュール９２に記憶されている。伸張部６６内の記憶モジュール１０６には、伸張部を特定するための個別ＩＤ、暗号処理部６５と相互認証する際に使用する共通鍵が、機器製造時に予

め記憶される。なお、暗号処理部６５と伸張部６６を１対１に対応させるため、それぞれの記憶モジュールに互いのＩＤを持たせておいても良い（相互認証が共通鍵で行われているため、結果的には対応した暗号処理部、伸張部でしかやりとりができない。但し処理としては公開鍵暗号方式の相互認証であっても良い。このとき保存されている鍵は共通鍵ではなく、伸張部６６固有の秘密鍵になる）。

【００８７】

外部メモリ６７には、コンテンツの復号を行う際に使用する保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}、そのコンテンツ鍵K_{co}を利用する際の条件を示す使用許諾条件情報が記憶されている。また、大容量記憶部６８には、記憶モジュール９２内にある機器個別の秘密鍵に対応する公開鍵の証明書（機器の公開鍵証明書）、登録情報、コンテンツプロバイダセキュアコンテナ（コンテンツ鍵K_{co}で暗号化されたコンテンツおよびその署名、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}およびその署名、配送鍵K_dで暗号化された個別鍵K_iおよびその署名、取扱方針およびその署名）、サービスプロバイダセキュアコンテナ（価格情報およびその署名）、コンテンツプロバイダ２の公開鍵証明書、サービスプロバイダ３の公開鍵証明書が記憶されている。

【００８８】

携帯機器５３には、ホームサーバ５１が保持する暗号処理部６５と同一の暗号処理部８３、外部メモリ６７と同一の外部メモリ８５が備えられている（内部データが同一のものは省略されている。例えば、伸張部）。しかし、その内部に保持されるデータは、図に示すように若干異なっている。暗号処理部８３内の記憶モジュールの保持するデータは、機器を特定するための個別ＩＤ、機器毎に異なる秘密鍵、保存鍵K_{save}、電子配信サービスセンタ１と相互認証する際に使用する、電子配信サービスセンタ１の公開鍵（ただし、ホームサーバ５１に電子配信サービスセンタ１との手続きを全て代行してもらう場合は必要ない）、公開鍵証明書を検証するための認証局２２の公開鍵、伸張部８４と相互認証する際に使用する共通鍵が記憶されている。これらのデータは、機器製造時に予め記憶されるデータである。また、外部メモリ８５内に保持するコンテンツ鍵K_{co}および使用許諾条件情報の改竄チェック用のハッシュ値、必要に応じて決済用ＩＤ、配送鍵

K_d、登録情報（の一部）（購入処理をしない場合、決済用ＩＤ、配送鍵K_dは必要ない）は、機器を使用し始めてから記憶されるデータであり、これらのデータも記憶されている（購入処理を行う場合、課金情報も記憶される）。外部メモリ８５には、暗号処理部８３内にある機器個別の秘密鍵に対応する公開鍵の証明書、コンテンツ鍵K_{co}で暗号化されたコンテンツおよびその署名（この他に、必要に応じて個別鍵K_iで暗号化されたコンテンツ鍵K_{co}およびその署名、配送鍵K_dで暗号化された個別鍵K_iおよびその署名必要に応じて、取扱方針およびその署名、価格情報およびその署名も記憶される場合がある）、コンテンツを復号化する際に使用する保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}、そのコンテンツを利用する際の条件を示す使用許諾条件情報が記憶されている。また、必要に応じてコンテンツプロバイダ２の公開鍵証明書、サービスプロバイダ３の公開鍵証明書も記憶されている。

【００８９】

据置機器５２には、ホームサーバ５１の構成に加え、記録メディア８０が備えられている。記録メディアとしては、通常のＭＤやＣＤ－Ｒの場合もあるし、電子配信専用の記憶メディアである場合もある。前者の場合、記憶されるデータはコピー禁止信号を付加された、復号化されたコンテンツになるが、勿論、暗号化されたコンテンツを入れておいてもよい（保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}も併せて記憶しておいても良い。この時、再生できるのは記憶した機器のみになる。なぜなら、保存鍵K_{save}は機器毎に異なっているからである）。

【００９０】

また、記憶メディアとしては、図１９が考えられる。電子配信専用記憶メディア１２０において、暗号処理部１２２内にある記憶モジュール１２５には、記録メディアの個別ＩＤ、記録メディア毎に異なる秘密鍵、この秘密鍵に対応する公開鍵の証明書（外部メモリ１２３に記録しておいても良い）、コンテンツ鍵K_{co}を暗号化するのに使用する保存鍵K_{save}（一般に、記憶メディア毎に異なる）、電子配信サービスセンタ１の公開鍵（センタとやりとりしない場合や外部メモリ１２３に電子配信サービスセンタ１の公開鍵証明書が有る場合には必要ない）、認証局の公開鍵、外部メモリ１２３の改竄を検査するためのハッシュ値、登録情

報（の一部）が記憶されている。外部メモリ１２３には、コンテンツ鍵K_{co}で暗号化されたコンテンツ（およびその署名）、保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}、使用許諾条件情報が記憶されており、必要に応じて取扱方針（およびその署名）、価格情報（およびその署名）、コンテンツプロバイダ２の公開鍵証明書、サービスプロバイダ３の公開鍵証明書が記憶されている。

【００９１】

図２０、図２１は、電子配信サービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信される情報を説明する図である。コンテンツプロバイダ２は、コンテンツプロバイダセキュアコンテナ（その詳細は後述する）にコンテンツプロバイダ２の公開鍵証明書（その詳細は後述する）を付して、サービスプロバイダ３に送信する。また、コンテンツプロバイダ２は、必要に応じて取扱方針およびその署名、コンテンツプロバイダ２の証明書を電子配信サービスセンタ１に送信する。

【００９２】

サービスプロバイダ３は、コンテンツプロバイダ２の公開鍵証明書を検証し、コンテンツプロバイダ２の公開鍵を入手し、受信したコンテンツプロバイダセキュアコンテナの署名を検証する（取扱方針のみ署名検証する場合もある）。署名の検証に成功した後、コンテンツプロバイダセキュアコンテナから取扱方針を取り出し、これを基に価格情報を生成し、価格情報に署名を付けてサービスプロバイダセキュアコンテナとする（その詳細は後述する）。コンテンツプロバイダセキュアコンテナ、サービスプロバイダセキュアコンテナ、コンテンツプロバイダ２の公開鍵証明書、およびサービスプロバイダ３の公開鍵証明書（その詳細は後述する）をユーザホームネットワーク５に送信する。また、サービスプロバイダ３は、必要に応じて価格情報およびその署名、サービスプロバイダ３の公開鍵証明書を電子配信サービスセンタ１に送信する。

【００９３】

ユーザホームネットワーク５は、受信したセキュアコンテナを検証した後、セキュアコンテナの中に含まれる取扱方針および価格情報に基づいて購入処理を行い、課金情報を生成して暗号処理部内の記憶モジュールに保存し、使用許諾条件

情報を生成し、コンテンツ鍵K_{co}を復号化して保存鍵K_{save}で再暗号化し、使用許諾条件情報および再暗号化されたコンテンツ鍵K_{co}を外部メモリ６７に保存しておく。そして、使用許諾条件情報に沿って、コンテンツ鍵K_{co}を保存鍵K_{save}で復号化し、この鍵でコンテンツを復号化して利用する。課金情報は、所定のタイミングで一時鍵K_{temp}で暗号化され、署名が付され、必要に応じて取扱方針および価格情報と共に電子配信サービスセンタ１に送信される。

【００９４】

電子配信サービスセンタ１は、課金情報および価格情報を基に使用料金を算出し、また電子配信サービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３それぞれの利益を算出する。電子配信サービスセンタ１は、さらに、コンテンツプロバイダ２から受信した取扱方針、サービスプロバイダ３から受信した価格情報、必要に応じて取扱方針、並びにユーザホームネットワーク５から受信した取扱方針、価格情報を比較し、サービスプロバイダ３またはユーザホームネットワーク５で取扱方針の改竄または不正な価格の付加等の不正がなかったか否か等の監視をする。

【００９５】

更に、電子配信サービスセンタ１は、コンテンツプロバイダ２にコンテンツプロバイダの公開鍵証明書を送信し、サービスプロバイダ３にサービスプロバイダの公開鍵証明書を送信する。また、工場出荷時に、各機器に応じて作成した公開鍵証明書を各機器に埋め込むため、各機器の公開鍵証明書に関するデータを工場に引き渡す。

【００９６】

図２２は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナ１Ａは、コンテンツ鍵K_{co}で暗号化されたコンテンツおよびその署名、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}およびその署名、配送鍵K_dで暗号化された個別鍵K_iおよびその署名、取扱方針および署名を含む。署名は、それぞれのデータにハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ２の秘密鍵K_{scp}を用いて生成されたデータである。なお、図２２の場合は鍵データ（個別鍵K_iで暗号化されたコンテンツ

鍵K_{CO}、配送鍵K_dで暗号化された個別鍵K_iに対してそれぞれ別々に署名を生成し付加するようにしたが、各鍵データ（個別鍵K_iで暗号化されたコンテンツ鍵K_{CO}、配送鍵K_dで暗号化された個別鍵K_i）を１つにまとめて１つの署名を生成し付加するようにしても良い。このように常に一体で使用される鍵データを１つにまとめて１つの署名を付加することにより、署名の検証が１回で済む。

【００９７】

図２３は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ１Ｂは、コンテンツ鍵K_{co}で暗号化されたコンテンツおよびその署名、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}およびその署名、取扱方針および署名を含む。

【００９８】

図２４は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ１Ｃは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}、配送鍵K_dで暗号化された個別鍵K_i、取扱方針、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}、配送鍵K_dで暗号化された個別鍵K_i、および取扱方針にハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ２の秘密鍵K_{scp}を用いて生成されたデータである。

【００９９】

図２５は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ１Ｄは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}、取扱方針、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}、および取扱方針にハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ２の秘密鍵K_{scp}を用いて生成されたデータである。

【０１００】

図２６は、コンテンツプロバイダ２の公開鍵証明書を説明する図である。コン

テンツプロバイダ２の公開鍵証明書２Ａは、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダ２の公開鍵K_{pcp}、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ２の名前、並びにコンテンツプロバイダ２の公開鍵K_{pcp}にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵K_{sca}を用いて生成したデータである。

【０１０１】

図２７は、コンテンツプロバイダ２の公開鍵証明書の他の例を説明する図である。コンテンツプロバイダ２の公開鍵証明書２Ｂは、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダ２の公開鍵K_{pcp}、配送鍵K_dで暗号化された個別鍵K_i、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダ２の公開鍵K_{pcp}、並びに配送鍵K_dで暗号化された個別鍵K_iにハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵K_{sca}を用いて生成したデータである。

【０１０２】

図２８は、コンテンツプロバイダ２の公開鍵証明書のまた別の例を説明する図である。　コンテンツプロバイダ２の公開鍵証明書２Ｃは、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダ２の

公開鍵K_{pcp}、個別鍵K_iの一部を配送鍵K_dで暗号化した、所定の種類のデータ、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダ２の公開鍵K_{pcp}、並びに個別鍵K_iの一部を配送鍵K_dで暗号化した、所定の種類のデータにハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵K_{sca}を用いて生成したデータである。

【０１０３】

図２９は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナ３Ａは、価格情報および署名で構成されている。署名は、価格情報に対し必要に応じてハッシュ関数を適用して生成されたハッシュ値に、サービスプロバイダ３の秘密鍵K_{ssp}を用いて生成されたデータである。

【０１０４】

図３０は、サービスプロバイダセキュアコンテナの他の例を説明する図である。サービスプロバイダセキュアコンテナ３Ｂは、コンテンツプロバイダセキュアコンテナ、価格情報、および署名を含む。署名は、コンテンツプロバイダセキュアコンテナ、および価格情報にハッシュ関数を適用して生成されたハッシュ値に、サービスプロバイダ３の秘密鍵K_{ssp}を用いて生成されたデータである。

【０１０５】

図３１は、サービスプロバイダ３の公開鍵証明書を説明する図である。サービスプロバイダ３の公開鍵証明書４Ａは、公開鍵証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダ３の公開鍵K_{psp}、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、サービスプロバイダ３の

名前、並びにサービスプロバイダ３の公開鍵K_{psp}にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵K_{sca}を用いて生成したデータである。

【０１０６】

図３２は、User機器の公開鍵証明書を説明する図である。User機器の公開鍵証明書５Ａは、公開鍵証明書のバージョン番号、認証局がUser機器（正確には暗号処理部（専用のＩＣチップ））に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、User機器の名前、User機器の公開鍵K_{pu}、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がUser機器に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、User機器の名前、並びにUser機器の公開鍵K_{pu}にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵K_{sca}を用いて生成したデータである。

【０１０７】

図３３および図３４は取扱方針のデータフォーマットを示すものであり、当該取扱方針はコンテンツプロバイダ２によりシングルコンテンツ毎、またアルバムコンテンツ毎に生成され、ユーザホームネットワーク５が購入可能な利用権の内容を示す。

【０１０８】

シングルコンテンツに対する取扱方針（図３３）のデータには、データの種別、取扱方針の種類、取扱方針の有効期限、コンテンツのＩＤ、コンテンツプロバイダのＩＤ、取扱方針のＩＤ、取扱方針のバージョン、地域コード、使用可能機器条件、使用可能User条件、サービスプロバイダのＩＤ、世代管理情報、当該取扱方針が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

【０１０９】

そして、ルールは、利用権毎に整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバ

イダの利益額、当該コンテンツプロバイダの利益率、データサイズ、送信情報から構成されている。

【０１１０】

また、アルバムコンテンツに対する取扱方針（図３４）のデータには、データの種別、取扱方針の種類、取扱方針の有効期限、アルバムのＩＤ、取扱方針のバージョン、コンテンツプロバイダのＩＤ、取扱方針のＩＤ、地域コード、使用可能機器条件、使用可能User条件、サービスプロバイダのＩＤ、当該アルバムを構成するシングルコンテンツの取扱方針の数、そのシングルコンテンツの取扱方針の格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたシングルコンテンツの取扱方針のデータパケット、世代管理情報、当該取扱方針が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

【０１１１】

そして、ルールは、シングルコンテンツの取扱方針のルールと同様に、利用権毎に整理番号として付けられたルール番号、利用権内容番号、パラメータ、最低販売価格、コンテンツプロバイダの利益額、当該コンテンツプロバイダの利益率、データサイズ、送信情報から構成されている。

【０１１２】

これら取扱方針において、データの種別はそのデータが取扱方針のデータであることを示し、取扱方針の種類は当該取扱方針がシングル又はアルバムコンテンツのいずれの取扱方針であるかを示している。取扱方針の有効期限は当該取扱方針の使用期間をその期限の切れる日付、又は使用を開始した基準となる日から期限の切れる日までの日数などによって示している。コンテンツのＩＤおよびアルバムのＩＤは取扱方針が示す購入可能なシングルコンテンツおよびアルバムコンテンツを示し、コンテンツプロバイダのＩＤは、当該取扱方針を規定したコンテンツプロバイダ２のＩＤを示している。

【０１１３】

また、取扱方針のＩＤは当該取扱方針を識別するためのものであり、例えば、

同一コンテンツに対して複数の取扱方針が設定された場合などに当該取扱方針を識別するために使用される。取扱方針のバージョンは使用期間に応じて改訂した取扱方針のその改訂情報を示している。従って、取扱方針はこれら取扱方針のＩＤおよび取扱方針のバージョンにより管理される。

【０１１４】

地域コードは取扱方針の使用可能な地域をコード化して示しており、当該地域コードには取扱方針の使用可能な地域を限定する特定の地域を示すコードと、当該取扱方針を全ての地域で使用可能にするコードを割り当てることができる。使用可能機器条件は取扱方針を利用し得る機器の条件を示し、使用可能User条件は取扱方針を利用し得るユーザの条件を示している。

【０１１５】

サービスプロバイダのＩＤは取扱方針を利用するサービスプロバイダ３のＩＤを示しており、当該サービスプロバイダのＩＤには取扱方針を使用し得るサービスプロバイダ３を限定する特定のサービスプロバイダ３のＩＤと、当該取扱方針を複数（全て）のサービスプロバイダで使用し得るようにするＩＤとがある。

【０１１６】

さらに、世代管理情報はコンテンツの再購入可能な最大回数を示す。署名は取扱方針から当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

【０１１７】

また、ルールにおいて、利用権内容番号は、利用権内容毎に付加された番号であり、パラメータは権利内容のパラメータを示す。最低販売価格は利用権内容に応じてシングルおよびアルバムコンテンツを販売する際の最低の販売価格を示し、コンテンツプロバイダの利益額および利益率はシングルコンテンツおよびアルバムコンテンツが購入されたときにコンテンツプロバイダ２が得ることのできる利益の金額および販売価格に対する利益率を示している。データサイズは送信情報のデータサイズを示し、当該送信情報は、コンテンツプロバイダ２が設定した、利用権の購入によりユーザに加算されるポイントや、当該ポイントに応じた利

用権の割引額でなるマイル情報や、必要に応じてコンテンツプロバイダ２が設定した各種情報からなる。

【０１１８】

ここで、アルバムコンテンツの取扱方針において、複数のルールは、当該アルバムの購入形態を示している。また、アルバムコンテンツの取扱方針に格納された複数のシングルコンテンツの取扱方針において、当該取扱方針に格納されたルールは、それぞれ対応するシングルコンテンツがアルバムのなかから、シングル曲として単独で購入し得る、又は対応するシングルコンテンツがアルバム曲としてのみ購入し得る（すなわち、アルバムとして、他のシングルコンテンツと共に一体化してしか購入し得ない）等のようにアルバム内におけるシングルコンテンツの購入形態を示している。

【０１１９】

従って、アルバムコンテンツの取扱方針においては、当該取扱方針のルールに基づいて、アルバムコンテンツを購入し、又はシングルコンテンツの取扱方針のルールに基づいて、シングルコンテンツをシングル曲として購入するように、アルバムコンテンツと、シングル曲として販売し得るシングルコンテンツとのいずれも選択して購入し得るように定義されている。

【０１２０】

また、アルバムコンテンツの取扱方針においては、全体に対して署名を付けたことにより、当該署名を検証するだけで、この取扱方針に格納したシングルコンテンツの取扱方針の署名をそれぞれ検証しなくてもこのアルバムコンテンツの取扱方針と共に、各シングルコンテンツの取扱方針に対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

【０１２１】

因みに、シングルおよびアルバムコンテンツの取扱方針には、必要に応じて、コンテンツに対する署名の検証を実行するか否かを示す署名の検証の有無を格納し得る。これは、コンテンツのデータ量が比較的多く、署名の検証に時間がかかるためであり、取扱方針にかかる署名の検証の有無の情報が格納された場合には、当該情報に従ってコンテンツの署名の検証を実行し、又は当該検証を実行しな

いようにする。

【０１２２】

また、アルバムコンテンツの取扱方針においては、当該アルバムを構成する複数のシングルコンテンツの取扱方針を格納しているものの、これら複数のシングルコンテンツの取扱方針を格納しなくても良い。

【０１２３】

さらに、シングルおよびアルバムコンテンツの取扱方針においては、コンテンツプロバイダの利益額および利益率を電子配信サービスセンタ１により一括管理しても良いため、図３５および図３６に示すように、これらコンテンツプロバイダの利益額および利益率を除いて構成しても良い。

【０１２４】

図３７および図３８は価格情報のデータフォーマットを示すものであり、当該価格情報はサービスプロバイダ３において、コンテンツプロバイダ２から与えられるシングルコンテンツの取扱方針毎、またアルバムコンテンツの取扱方針毎に生成され、シングルコンテンツおよびアルバムコンテンツの価格を示す。

【０１２５】

シングルコンテンツに対する価格情報（図３７）のデータには、データの種別、価格情報の種類、価格情報の有効期限、コンテンツのＩＤ、サービスプロバイダのＩＤ、価格情報のＩＤ、価格情報のバージョン、地域コード、使用可能機器条件、使用可能User条件、コンテンツプロバイダのＩＤ、当該価格情報が付加された取扱方針のＩＤ、当該価格情報が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

【０１２６】

そして、ルールは利用権毎に整理番号として付けられたルール番号、サービスプロバイダの利益額、当該サービスプロバイダの利益率、価格、データサイズ、送信情報から構成されている。

【０１２７】

また、アルバムコンテンツに対する価格情報（図３８）のデータには、データ

の種別、価格情報の種類、価格情報の有効期限、アルバムのＩＤ、サービスプロバイダのＩＤ、価格情報のＩＤ、価格情報のバージョン、地域コード、使用可能機器条件、使用可能User条件、コンテンツプロバイダのＩＤ、当該価格情報が付加された取扱方針のＩＤ、当該アルバムを構成するシングルコンテンツの価格情報の数、そのシングルコンテンツの価格情報の格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたシングルコンテンツの価格情報のデータパケット、当該価格情報が示す購入可能な利用権を含むルールの数、そのルールの格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

【０１２８】

そして、ルールは、シングルコンテンツに対する価格情報のルールと同様に、利用権毎に整理番号として付けられたルール番号、サービスプロバイダの利益額、当該サービスプロバイダの利益率、価格、データサイズ、送信情報から構成されている。

【０１２９】

これら価格情報において、データの種別はこのデータが価格情報のデータであることを示し、価格情報の種類は当該価格情報がシングルコンテンツ又はアルバムコンテンツのいずれの価格情報であるかを示している。価格情報の有効期限は当該価格情報の使用期間をその期限の切れる日付、又は使用開始の基準となる日から期限の切れる日までの日数などによって示している。コンテンツのＩＤおよびアルバムのＩＤは価格情報が示す購入可能なシングルコンテンツおよびアルバムコンテンツを示し、サービスプロバイダのＩＤは当該価格情報を作成したサービスプロバイダ３のＩＤを示している。

【０１３０】

また、価格情報のＩＤは当該価格情報を識別するためのものであり、例えば、同一コンテンツに対して複数の価格情報が設定された場合などに当該価格情報を識別するために使用される。価格情報のバージョンは使用期間に応じて改訂された価格情報の改訂情報を示している。従って、価格情報はこれら価格情報のＩＤおよび価格情報のバージョンにより管理される。

【０１３１】

地域コードは価格情報の使用可能な地域をコード化して示しており、当該地域コードには価格情報の使用可能な地域を限定する特定の地域を示すコードと、当該価格情報を全ての地域で使用可能にするコードを割り当てることができる。使用可能機器条件は価格情報を利用し得る機器の条件を示し、使用可能User条件は価格情報を利用し得るユーザの条件を示している。コンテンツプロバイダのＩＤは価格情報を付加した取扱方針を規定したコンテンツプロバイダ２のＩＤを示している。取扱方針のＩＤは価格情報を付加した取扱方針を識別するためのものである。

【０１３２】

さらに、署名は価格情報から当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

【０１３３】

また、ルールにおいて、ルール番号は対応する取扱方針が示すルールのルール番号をそのまま用いる。サービスプロバイダの利益額および利益率はシングルコンテンツおよびアルバムコンテンツが購入されたときにサービスプロバイダ３が得ることのできる利益の金額および価格に対する利益率を示し、価格はサービスプロバイダ３により利用権内容および対応する最低販売価格に基づいて設定されたシングルコンテンツおよびアルバムコンテンツの販売価格を示す。データサイズは送信情報のデータサイズを示し、当該送信情報は、サービスプロバイダ３が設定した、利用権の購入によりユーザに加算されるポイントや、当該ポイントに応じた利用権の割引額でなるマイル情報や、必要に応じてサービスプロバイダ３が設定した各種情報からなる。

【０１３４】

ここで、サービスプロバイダ３は、価格情報を生成する際、対応する取扱方針が示す購入可能な全ての利用権を当該価格情報が示す購入可能な利用権として設定することができると共に、当該取扱方針が示す購入可能な全ての利用権のうち

から任意に選定した利用権を価格情報が示す購入可能な利用権として設定することもでき、コンテンツプロバイダ２が規定した利用権を選定し得る。

【０１３５】

また、アルバムコンテンツの価格情報において、複数のルールは、アルバムの購入形態に応じた販売価格を規定している。また、アルバムコンテンツの価格情報に格納された複数のシングルコンテンツの価格情報のうち、シングル曲として販売し得るシングルコンテンツの価格情報のルールは、当該シングル曲として販売し得るシングルコンテンツの販売価格を規定している。

【０１３６】

従って、アルバムコンテンツの価格情報においては、当該価格情報１つでアルバムの販売価格と、シングル曲として販売し得るシングルコンテンツの販売価格とを認識し得るようになされている。

【０１３７】

また、アルバムコンテンツの価格情報においては、全体に対して署名を付けたことにより、当該署名を検証するだけで、この価格情報に格納したシングルコンテンツの価格情報の署名をそれぞれ検証しなくてもこのアルバムコンテンツの価格情報と共に、各シングルコンテンツの価格情報に対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

【０１３８】

因みに、シングルおよびアルバムの価格情報においては、図３３および図３４について上述した取扱方針と同様にコンテンツに対する署名の検証の有無を格納し得る。また、アルバムコンテンツの価格情報においては、当該アルバムを構成する複数のシングルコンテンツの価格情報を格納しているものの、これら複数のシングルコンテンツの価格情報を格納しなくても良い。

【０１３９】

さらに、シングルおよびアルバムコンテンツの価格情報においては、サービスプロバイダの利益額および利益率を電子配信サービスセンタ１により一括管理しても良いため、図３９および図４０に示すように、これらサービスプロバイダの利益額および利益率を除いて構成しても良い。

【０１４０】

図４１は使用許諾条件情報のデータフオーマットを示すものであり、当該使用許諾条件情報はユーザホームネットワーク５内の機器において、ユーザがコンテンツを購入した際、当該購入したコンテンツの取扱方針に基づいて作成され、この取扱方針の示す利用権内容のうちのユーザが選択した利用権内容を示す。

【０１４１】

使用許諾条件情報のデータには、データの種別、使用許諾条件情報の種類、使用許諾条件情報の有効期限、コンテンツのＩＤ、アルバムのＩＤ、暗号処理部のＩＤ、ユーザのＩＤ、コンテンツプロバイダのＩＤ、取扱方針のＩＤ、取扱方針のバージョン、サービスプロバイダのＩＤ、価格情報のＩＤ、価格情報のバージョン、使用許諾条件情報のＩＤ、再生権（利用権）に整理番号として付けられたルール番号、利用権内容番号、再生残り回数、再生権の有効期限、複製権（利用権）に整理番号として付けられたルール番号、利用権内容番号、複製の残り回数、世代管理情報、再生権を保有する暗号処理部のＩＤが格納されている。

【０１４２】

使用許諾条件情報において、データの種別はこのデータが使用許諾条件情報のデータであることを示し、使用許諾条件情報の種類は当該使用許諾条件情報がシングルコンテンツ又はアルバムコンテンツのいずれの使用許諾条件情報であるかを示している。使用許諾条件情報の有効期限は当該使用許諾条件情報の使用期間をその期限の切れる日付、又は使用開始の基準となる日から期限の切れる日までの日数などによって示している。

【０１４３】

コンテンツのＩＤには購入されたシングルコンテンツを示すＩＤが記述され、アルバムのＩＤにはアルバムが購入されたときのみ当該アルバムを示すＩＤが記述される。実際には、コンテンツがシングルとして購入された場合、コンテンツのＩＤのみに購入されたシングルコンテンツを示すＩＤが記述され、また、コンテンツがアルバムとして購入された場合には、コンテンツのＩＤに、アルバムを構成する全てのシングルコンテンツのＩＤが記述され、かつアルバムのＩＤに購入されたアルバムを示すＩＤが記述される。従って、このアルバムのＩＤをみれ

ば、購入されたコンテンツがシングルであるか、又はアルバムであるかを容易に判断し得る。

【０１４４】

暗号処理部のＩＤはコンテンツを購入処理したユーザホームネットワーク５内の機器の暗号処理部を示す。ユーザのＩＤはコンテンツを購入したユーザホームネットワーク５内の機器を複数のユーザが共有しているときに、当該機器を共有する複数のユーザを示している。

【０１４５】

また、コンテンツプロバイダのＩＤは使用許諾条件情報を作成するために用いた取扱方針を規定したコンテンツプロバイダ２のＩＤを示し、取扱方針のＩＤは当該使用許諾条件情報を作成するために用いた取扱方針を示す。取扱方針のバージョンは使用許諾条件情報を作成するために用いた取扱方針の改訂情報を示している。サービスプロバイダのＩＤは使用許諾条件情報を作成するために用いた価格情報を作成したサービスプロバイダ３のＩＤを示し、価格情報のＩＤは当該使用許諾条件情報を作成するために用いた価格情報を示す。価格情報のバージョンは使用許諾条件情報を作成するために用いた取扱方針の改訂情報を示している。従って、これらコンテンツプロバイダのＩＤ、取扱方針のＩＤ、取扱方針のバージョン、サービスプロバイダのＩＤ、価格情報のＩＤおよび価格情報のバージョンにより、ユーザが購入したコンテンツを提供したコンテンツプロバイダ２又はサービスプロバイダ３を知り得るようになされている。

【０１４６】

使用許諾条件情報のＩＤはコンテンツを購入したユーザホームネットワーク５内の機器の暗号処理部が付けるものであり、当該使用許諾条件情報を識別するために使用される。再生権のルール番号は利用権のうちの再生権に付けられた整理番号を示し、対応する取扱方針および価格情報が示すルールのルール番号をそのまま用いる。利用権内容は後述する再生権の内容を示す。再生残り回数は購入したコンテンツに対して予め設定された再生回数のうちの残りの再生回数を示し、再生権の有効期限は購入したコンテンツの対する再生可能期間をその期限の切れる日時などによって示している。

【０１４７】

また、複製権のルール番号は利用権のうちの複製権に付けられた整理番号を示し、対応する取扱方針および価格情報が示すルールのルール番号をそのまま用いる。利用権内容は後述する複製権の内容を示す。複製残り回数は購入したコンテンツに対して予め設定された複製回数のうちの残りの複製回数を示す。

【０１４８】

さらに、世代管理情報はコンテンツを再購入した際に当該コンテンツの再購入可能な残り回数を示す。再生権を保有する暗号処理部のＩＤは現時点において再生権を保有する暗号処理部を示しており、管理移動したときには再生権を保有する暗号処理部のＩＤが変更される。

【０１４９】

因みに、使用許諾条件情報においては、複製権に対して有効期限を規定しても良く、当該有効期限を規定した場合には購入したコンテンツの対する複製可能期間をその期限の切れる日時などによって示す。

【０１５０】

図４２は課金情報を示すものであり、当該課金情報はユーザホームネットワーク５内の機器により、コンテンツの購入の際に、当該コンテンツに対応する取扱方針および価格情報に基づいて生成される。

【０１５１】

課金情報のデータには、データの種別、暗号処理部のＩＤ、ユーザのＩＤ、コンテンツのＩＤ、コンテンツプロバイダのＩＤ、取扱方針のＩＤ、取扱方針のバージョン、サービスプロバイダのＩＤ、価格情報のＩＤ、価格情報のバージョン、使用許諾条件情報のＩＤ、ルール番号、コンテンツプロバイダ２の利益額および利益率、サービスプロバイダの利益額および利益率、世代管理情報、コンテンツプロバイダの設定した送信情報のデータサイズ、そのコンテンツプロバイダの設定した送信情報、サービスプロバイダの設定した送信情報のデータサイズ、そのサービスプロバイダの設定した送信情報、供給元のＩＤが格納されている。

【０１５２】

課金情報において、データの種別は当該データが課金情報であることを示し、

暗号処理部のＩＤは、コンテンツの購入処理を実行して当該課金情報を生成した機器の暗号処理部を示す。ユーザのＩＤはコンテンツを購入したユーザホームネットワーク５内の機器を複数のユーザが共有しているときに、当該機器を共有する複数のユーザを示し、コンテンツのＩＤは当該購入されたコンテンツ（シングルコンテンツ又はアルバムコンテンツ）を示す。

【０１５３】

また、コンテンツプロバイダのＩＤは購入処理に用いた取扱方針を規定したコンテンツプロバイダ２のＩＤ（この取扱方針に含まれるコンテンツプロバイダのＩＤ）を示し、取扱方針のＩＤは当該購入処理に用いた取扱方針を示す。取扱方針のバージョンは、購入処理に用いた取扱方針の改訂情報を示す。サービスプロバイダのＩＤは購入処理に用いた価格情報を作成したサービスプロバイダ３のＩＤ（この価格情報に含まれるサービスプロバイダのＩＤ）を示し、価格情報のＩＤは当該購入処理に用いた価格情報を示す。価格情報のバージョンは、購入処理に用いた価格情報の改訂情報を示す。

【０１５４】

使用許諾条件情報のＩＤは購入処理の際に作成した使用許諾条件情報のＩＤを示し、ルール番号は購入された利用権に整理番号として付けられたルール番号を示す。コンテンツプロバイダの利益額および利益率はコンテンツの購入によりコンテンツプロバイダ２に分配される配当の金額および売上に対する割合を示し、サービスプロバイダの利益額および利益率は当該コンテンツの購入によりサービスプロバイダ３に分配される配当の金額および売上に対する割合を示す。

【０１５５】

さらに、世代管理情報は購入されたコンテンツの世代を示す。また、コンテンツプロバイダの設定した送信情報のデータサイズおよびそのコンテンツプロバイダの設定した送信情報には、購入処理に用いた取扱方針が示すデータサイズと、送信情報をそのまま格納すると共に、サービスプロバイダの設定した送信情報のデータサイズおよびそのサービスプロバイダの設定した送信情報には購入処理に用いた価格情報が示すデータサイズと、送信情報をそのまま格納する。そして、供給元のＩＤは、購入処理したコンテンツの供給元の機器を示し、このＩＤはコ

ンテンツの再購入が行われる毎に累積される。

【０１５６】

因みに、課金情報においては、コンテンツプロバイダの利益額および利益率と、サービスプロバイダの利益額および利益率を電子配信サービスセンタ１により一括管理しても良いため、図４３に示すように、これらコンテンツプロバイダの利益額および利益率およびサービスプロバイダの利益額および利益率を除いて構成しても良い。

【０１５７】

図４４は購入可能な利用権の内容を示したものであり、当該利用権としては、大きく分けて再生権、複製権、権利内容変更権、再購入権、追加購入権、管理移動権がある。

【０１５８】

再生権には、期間制限および回数制限のない無制限再生権と、再生期間を制限する期間制限付き再生権、再生の積算時間を制限する積算時間制限付き再生権、再生回数を制限する回数制限付き再生権がある。複製権には、期間制限、回数制限およびコピー管理情報（例えば、シリアルコピーマネージメント：SCMS）のないコピー管理情報なし無制限複製権、複製回数を制限するもののコピー管理情報のない回数制限付きおよびコピー管理情報なし複製権、期間制限および回数制限はないもののコピー管理情報を付加して提供するコピー管理情報付き複製権、複製回数を制限し、かつコピー管理情報を付加して提供する回数制限およびコピー管理情報付き複製権がある。因みに、複製権としては、この他に複製可能期間を制限する期間制限付き複製権（コピー管理情報を付加するものと、当該コピー管理情報を付加しないものとがある）や、複製の積算時間（すなわち、複製されたコンテンツの再生に要する積算時間）を制限する積算時間制限付き複製権（コピー管理情報を付加するものと、当該コピー管理情報を付加しないものとがある）等がある。

【０１５９】

また、権利内容変更権は上述したように既に購入した利用権の内容を別の内容に変更する権利であり、再購入権も上述したように他の機器で購入した権利に基

づき利用権を別途購入する権利である。追加購入権は、既に単独で購入したコンテンツに当該コンテンツを含むアルバムの他のコンテンツを追加購入してアルバム化する権利であり、管理移動権は購入した利用権を移動して保有者を変更する権利である。

【０１６０】

次に、図３３などに示されている利用権内容の具体例を説明する。実際に、無制限再生権のデータとしては、図４５（Ａ）に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報が利用権内容の領域に格納される。期間制限付き再生権のデータとしては、図４５（Ｂ）に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報が利用権内容の領域に格納される。

【０１６１】

積算時間制限付き再生権のデータとしては、図４５（Ｃ）に示すように再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報と、再生し得る積算時間の制限を示す日数および時間の情報とが利用権内容の領域に格納される。回数制限付き再生権のデータとしては、図４５（Ｄ）に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報と、再生し得る回数を示す再生回数の情報とが利用権内容の領域に格納される。

【０１６２】

また、コピー管理情報なし無制限複製権のデータとしては、図４５（Ｅ）に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報が利用権内容の領域に格納されている。回数制限付きおよびコピー管理情報なし複製権のデータとしては、図４５（Ｆ）に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日

までの日数などによって示す当該複製権の有効期限の情報と、複製し得る回数を示す複製回数の情報とが利用権内容の領域に格納される。

【０１６３】

コピー管理情報付き複製権のデータとしては、図４５（Ｇ）に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報が利用権内容の領域に格納されている。回数制限およびコピー管理情報付き複製権のデータとしては、図４５（Ｈ）に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報と、複製し得る回数を示す複製回数の情報とが利用権内容の領域に格納される。

【０１６４】

さらに、権利内容変更権のデータとしては、図４５（Ｉ）に示すように、当該権利内容変更権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該権利内容変更権の有効期限の情報と、変更前の利用権内容を検索するための旧ルール番号と、変更後の利用権内容を検索するための新ルール番号とが利用権内容の領域に格納される。因みに、利用権内容として、例えば、期間制限付き再生権１つをみても、その期間の設定により複数種類の期間制限付き再生権が存在するように、利用権内容毎に複数種類の内容が存在する。従って、利用権内容を利用権内容番号だけでは管理し難いため、権利内容変更権においては、これら利用権内容毎の複数の内容毎に付けられたルール番号により利用権内容を管理する。

【０１６５】

再購入権のデータとしては、図４５（Ｊ）に示すように、当該再購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再購入権の有効期限の情報と、再購入前の利用権内容を検索するための旧ルール番号と、再購入後の利用権内容を検索するための新ルール番号と、再購入し得る最大回数の示す最大配信世代情報とが利用権内容の領域に格納される。

【０１６６】

追加購入権のデータとしては、図４５（Ｋ）に示すように、当該追加購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該追加購入権の有効期限の情報と、アルバムコンテンツを構成する複数のシングルコンテンツのうちの既に購入したシングルのコンテンツを示す最小保有コンテンツ番号および最大保有コンテンツ番号とが利用権内容の領域に格納される。

【０１６７】

管理移動権のデータとしては、図４５（Ｌ）に示すように、当該管理移動権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該管理移動権の有効期限の情報が利用権内容の領域に格納される。

【０１６８】

因みに、かかる利用権内容として、例えば、ゲームのデータを複数のコンテンツに分割した際にこれらコンテンツを所定の順番に従って購入するためのコンテンツ購入権を規定しても良い。そして、コンテンツ購入権のデータとしては、図４５（Ｍ）に示すように、当該コンテンツ購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該コンテンツ購入権の有効期限の情報と、既に購入されているコンテンツのＩＤと、既に購入された利用権内容を検索するための旧ルール番号と、新たに購入する利用権内容を検索するための新ルール番号とを利用権内容の領域に格納する。このようにすることで、連続したストーリーをもつゲームプログラムなどを、ユーザに連続して購入させるようにしたり、また、コンテンツ（ゲーム）そのものをアップグレードし得る。

【０１６９】

図４６はシングルコンテンツのデータフォーマットを示すものであり、当該シングルコンテンツのデータには、データの種別、コンテンツの種類、コンテンツの有効期限、コンテンツのカテゴリー、コンテンツのＩＤ、コンテンツプロバイダのＩＤ、コンテンツの暗号方式、暗号化したコンテンツのデータ長、その暗号

したコンテンツ、公開鍵証明書、署名が格納されている。

【０１７０】

このシングルコンテンツにおいて、データの種別はそのデータがコンテンツのデータであることを示し、コンテンツの種類は当該コンテンツがシングルであることを示す。コンテンツの有効期限は当該コンテンツの配信期限をこの期限の切れる日付、又は配信を開始した基準となる日から期限の切れる日までの日数などによって示している。コンテンツのカテゴリーは当該コンテンツが音楽データ、プログラムデータ、映像データなどのいずれのカテゴリーのものであるかを示し、コンテンツのＩＤはこのシングルコンテンツを識別するためのものである。

【０１７１】

コンテンツプロバイダのＩＤは、このシングルコンテンツを保有するコンテンツプロバイダ２のＩＤを示す。コンテンツの暗号方式は当該コンテンツの暗号に用いる暗号方式（例えば、DES ）を示す。署名はシングルコンテンツのデータから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

【０１７２】

また、図４７はアルバムコンテンツのデータフォーマットを示すものであり、当該アルバムコンテンツのデータには、データの種別、コンテンツの種類、コンテンツの有効期限、アルバムのＩＤ、コンテンツプロバイダのＩＤ、シングルコンテンツの数、シングルコンテンツのアドレス情報、シングルコンテンツ、公開鍵証明書、署名が格納されている。

【０１７３】

このアルバムコンテンツにおいて、データの種別はそのデータがコンテンツのデータであることを示し、コンテンツの種類は当該コンテンツがアルバムであることを示す。コンテンツの有効期限は当該コンテンツの配信期限をこの期限の切れる日付、又は配信を開始した基準となる日から期限の切れる日までの日数などによって示し、アルバムのＩＤはこのアルバムコンテンツを識別するためのものである。

【０１７４】

コンテンツプロバイダのＩＤは、このアルバムコンテンツを保有するコンテンツプロバイダ２のＩＤを示す。シングルコンテンツの数はアルバムを構成するシングルコンテンツの数を示し、シングルコンテンツのアドレス情報は当該アルバムを構成するシングルコンテンツの格納位置を示し、そして、シングルコンテンツは当該アドレス情報の示す位置に実際に格納された、このアルバムを構成する複数のシングルコンテンツのデータパケットである。また、署名はアルバムコンテンツのデータから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

【０１７５】

そして、アルバムコンテンツにおいては、全体に対して署名を付けたことにより、当該署名を検証するだけで、このアルバムコンテンツに格納したシングルコンテンツの署名をそれぞれ検証しなくても当該アルバムコンテンツと共に、各シングルコンテンツに対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

【０１７６】

図４８はシングルコンテンツ用の鍵のデータフォーマットを示すものであり、当該シングルコンテンツ用の鍵データには、データの種別、鍵データの種類、鍵の有効期限、コンテンツのＩＤ、コンテンツプロバイダのＩＤ、鍵のバージョン、コンテンツ鍵K_{co}の暗号方式、暗号化されたコンテンツ鍵K_{co}、個別鍵K_iの暗号方式、暗号化された個別鍵K_i、公開鍵証明書、署名が格納されている。

【０１７７】

シングルコンテンツ用の鍵データにおいて、データの種別はこのデータが鍵のデータであることを示し、鍵データの種類は当該鍵データがシングルコンテンツ用であることを示す。鍵の有効期限は鍵データに示す鍵（コンテンツ鍵K_{co}および個別鍵K_i）の使用期間をその期限の切れる日付、又は鍵の使用を開始した基準となる日から期限の切れる日までの日数などによって示し、コンテンツのＩＤはコンテンツ鍵K_{co}により暗号化するシングルコンテンツを示す。コンテンツプ

ロバイダのＩＤはコンテンツを保有し、かつコンテンツ鍵K_{co}を生成したコンテンツプロバイダ２のＩＤを示す。

【０１７８】

鍵のバージョンは使用期間に応じて改訂された鍵（コンテンツ鍵K_{co}および個別鍵K_i）の改訂情報を示す。コンテンツ鍵K_{co}の暗号方式は個別鍵K_iを用いてコンテンツ鍵K_{co}を暗号化する際の暗号方式（例えば、DES）を示し、暗号化されたコンテンツ鍵K_{co}はその暗号方式により個別鍵K_iを用いて暗号化されたコンテンツ鍵K_{co}を示す。個別鍵K_iの暗号化方式は配送鍵K_dを用いて個別鍵K_iを暗号化する際の暗号方式（例えば、Triple-DES-CBC）を示し、暗号化された個別鍵K_iはその暗号方式により配送鍵K_dを用いて暗号化された個別鍵K_iを示す。署名はシングルコンテンツ用の鍵データから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

【０１７９】

ここで、配送鍵K_dおよび個別鍵K_iはコンテンツプロバイダ２からシングルコンテンツ用の鍵データにより常に一体にされて配送される。そして、シングルコンテンツ用の鍵データにおいては、その全体に対して１つの署名が付加されている。従って、シングルコンテンツ用の鍵データを受け取った機器においては、暗号化されたコンテンツ鍵K_{co}および暗号化された個別鍵K_iに対してそれぞれ別々に署名を検証する必要がなく、シングルコンテンツ用の鍵データの１つの署名を検証するだけで当該暗号化されたコンテンツ鍵K_{co}および暗号化された個別鍵K_iに対する署名の検証をしたことになり、かくして、これら暗号化されたコンテンツ鍵K_{co}および暗号化された個別鍵K_iに対する署名の検証を簡易化し得る。

【０１８０】

因みに、個別鍵K_iは、当該個別鍵K_iを用いてコンテンツ鍵K_{co}を暗号化するコンテンツプロバイダのＩＤと共に暗号化される。実際に、トリプルデスのＣＢＣモードと呼ばれる暗号化方式によってコンテンツプロバイダのＩＤと共に個

別鍵K_iを暗号化する方法を図４９を用いて説明する。すなわち、かかる暗号化方式では、所定の初期値と、個別鍵K_i（64bit）とを連接した後、配送鍵K_dを用いてトリプルデスのＣＢＣモードによる暗号化方式で暗号化し、この結果、得られた64bit の第１の値をコンテンツプロバイダのＩＤ（64bit）と連接した後、再び配送鍵K_dを用いてトリプルデスのＣＢＣモードによる暗号化方式で暗号化し、かくして、64bit の第２の値を得る。そして、かかる暗号化方式では、第１の値と第２の値とを連接した16バイトのデータが、シングルコンテンツ用の鍵データに格納される暗号化された個別鍵K_iとなる（この場合、第１の値はシングルコンテンツ用の鍵データに格納される暗号化された個別鍵K_iの始めの64bit のデータに相当し、また、第２の値は当該シングルコンテンツ用の鍵データに格納される暗号化された個別鍵K_i内の第１の値に続く64bit のデータとなる）。

【０１８１】

また、図５０はアルバムコンテンツ用の鍵データを示すものであり、当該アルバムコンテンツ用の鍵データには、データの種別、鍵データの種類、鍵の有効期限、アルバムのＩＤ、コンテンツプロバイダのＩＤ、鍵のバージョン、アルバムを構成するシングルコンテンツの暗号化の際に用いるシングルコンテンツ用の鍵データの数、その鍵データの格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納された鍵データパケット、公開鍵証明書、署名が格納されている。

【０１８２】

アルバムコンテンツ用の鍵データにおいて、データの種別はこのデータが鍵のデータであることを示し、鍵データの種類は当該鍵データがアルバムコンテンツ用であることを示す。鍵の有効期限は鍵データに示す鍵（コンテンツ鍵K_{co}）の使用期間をその期限の切れる日付、又は鍵の使用を開始した基準となる日から期限の切れる日までの日数などによって示し、アルバムのＩＤはコンテンツ鍵K_{co}により暗号化するシングルコンテンツからなるアルバムコンテンツを示す。コンテンツプロバイダのＩＤはアルバムコンテンツを暗号化するコンテンツプロバイダ２のＩＤを示す。

【０１８３】

鍵のバージョンは使用期間に応じて改訂された鍵（コンテンツ鍵K_{co}）の改訂情報を示す。署名はシングルコンテンツ用の鍵データから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

【０１８４】

そして、アルバムコンテンツ用の鍵データにおいては、全体に対して署名を付けたことにより、当該署名を検証するだけで、当該アルバムコンテンツ用の鍵データに格納した複数のシングルコンテンツ用の鍵データの署名をそれぞれ検証しなくても当該アルバムコンテンツ用の鍵データと共に、各シングルコンテンツ用の鍵データに対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

【０１８５】

図５１は、１つの共通鍵で、共通鍵暗号であるＤＥＳを用いる、暗号処理部６５と伸張部６６との相互認証の動作を説明する図である。図５１において、Ａを伸張部６６、Ｂを暗号処理部６５とすると、暗号処理部６５は６４ビットの乱数R_Bを生成し、R_Bおよび自己のＩＤであるID_Bを、上位コントローラ６２を介して伸張部６６に送信する。これを受信した伸張部６６は、新たに６４ビットの乱数R_Aを生成し、R_A、R_B、ID_BをＤＥＳのＣＢＣモードで鍵K_{AB}を用いて暗号化し、上位コントローラ６２を介して暗号処理部６５に返送する。

【０１８６】

ＤＥＳのＣＢＣモードとは、暗号化する際に、一つ前の出力と入力を排他的論理和し、それから暗号化する手法である。本例で言うならば、

$X = DES(K_{AB}, R_A + IV)$　ＩＶ＝初期値、＋：排他的論理和

$Y = DES(K_{AB}, R_B + X)$

$Z = DES(K_{AB}, ID_B + Y)$

となり、出力は、Ｘ、Ｙ、Ｚとなる。これらの式において、$DES(K_{AB}, R_A + IV)$は鍵K_{AB}を使ってデータ$R_A + IV$をＤＥＳで暗号化することを表し、

ＤＥＳ（K_{AB}、R_B＋Ｘ）は鍵K_{AB}を使ってデータR_B＋ＸをＤＥＳで暗号化することを表し、ＤＥＳ（K_{AB}、ID_B＋Ｙ）は鍵K_{AB}を使ってデータID_B＋ＹをＤＥＳで暗号化することを表す。

【０１８７】

これを受信した暗号処理部６５は、受信データを鍵K_{AB}で復号化し、R_BおよびID_Bが、暗号処理部６５が送信したものと一致するか検査する。この検査に通った場合、伸張部６６を正当なものとして認証する。続けて、セッション鍵（一時鍵K_{temp}のこと、乱数により生成する）SK_{AB}を生成し、R_B、R_A、SK_{AB}をＤＥＳのＣＢＣモードで鍵K_{AB}を用いて暗号化し、上位コントローラ６２を介して伸張部６６に送信する。これを受信した伸張部６６は、受信データを鍵K_{AB}で復号化し、R_BおよびR_Aが、伸張部６６が送信したものと一致するか検査する。この検査に通った場合、暗号処理部６５を正当なものとして認証し、データSK_{AB}をセッション鍵として以降の通信に使用する。なお、受信データの検査の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１８８】

図５２は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、ホームサーバ５１の暗号処理部６５内の相互認証モジュール９５と据置機器５２の暗号処理部７３内の図示せぬ相互認証モジュールとの相互認証の動作を説明する図である。図５２において、Ａを暗号処理部７３、Ｂを暗号処理部６５とすると、暗号処理部６５は、６４ビットの乱数R_Bを生成し、上位コントローラ６２、通信部６１を介して据置機器５２へ送信する。これを受信した据置機器５２は、暗号処理部７３において新たに６４ビットの乱数R_A、および標数ｐより小さい乱数A_Kを生成する。そして、ベースポイントＧをA_K倍した点A_Vを求め、R_A、R_B、A_V（Ｘ座標とＹ座標）を連接し（６４ビット＋６４ビット＋１６０ビット＋１６０ビットで、４４８ビットになる）、そのデータに対し、自己の持つ秘密鍵で署名データＡ．Ｓｉｇを生成する。なお、ベースポイントのスカラー倍は図１０の署名の生成で説明した方法と同じであるためその説明は省略する。データの連接とは、例えば次のようになる。１６ビットのデータＡと１６ビットの

データＢを連接すると、上位１６ビットのデータがＡで、下位１６ビットのデータがＢになる３２ビットのデータのことを言う。署名の生成は図１０の署名の生成で説明した方法と同じであるためその説明は省略する。

【０１８９】

次に、暗号処理部７３は、R_A、R_B、A_Vおよび署名データＡ．Ｓｉｇを上位コントローラ７２に引き渡し、上位コントローラ７２は、据置機器５２用の公開鍵証明書（小容量記憶部７５に保存されている）を追加して通信部７１を介してホームサーバ５１に送信する。公開鍵証明書は図３２で説明しているのでその詳細は省略する。これを受信したホームサーバ５１は、暗号処理部６５において据置機器５２の公開鍵証明書の署名を検証する。署名の検証は、図１１の署名の検証で説明した方法と同じであるためその説明は省略する。次に、送られてきたデータのうち、乱数R_Bが、暗号処理部６５が送信したものと同一かどうか検査し、同一であった場合には署名データＡ．Ｓｉｇを検証する。検証に成功したとき、暗号処理部６５は暗号処理部７３を認証する。なお、署名の検証は図１１の署名の検証で説明した方法と同じであるためその説明は省略する。そして、暗号処理部６５は、標数ｐより小さい乱数B_Kを生成し、ベースポイントＧをB_K倍した点B_Vを求め、R_B、R_A、B_V（Ｘ座標とＹ座標）を連接し、そのデータに対し、自己の持つ秘密鍵で署名データＢ．Ｓｉｇを生成する。最後に、暗号処理部６５は、R_B、R_A、B_Vおよび署名データＢ．Ｓｉｇを上位コントローラ６２に引き渡し、上位コントローラ６２は、ホームサーバ５１用の公開鍵証明書（大容量記憶部６８に保存されている）を追加して通信部６１を介して据置機器５２に送信する。

【０１９０】

これを受信した据置機器５２は、暗号処理部７３においてホームサーバ５１の公開鍵証明書の署名を検証する。次に、送られてきたデータのうち、乱数R_Aが、暗号処理部７３が送信したものと同一かどうか検査し、同一であった場合には署名データＢ．Ｓｉｇを検証する。検証に成功したとき、暗号処理部７３は暗号処理部６５を認証する。

【０１９１】

両者が認証に成功した場合には、暗号処理部６５はB_K A_V（B_Kは乱数だが、A_Vは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、暗号処理部７３はA_K B_Vを計算し、これら点のＸ座標の下位６４ビットをセッション鍵（一時鍵K_{temp}）として以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。因に、通信に使用するセッション鍵としては、Ｘ座標の下位６４ビットに限らず、Ｙ座標の下位６４ビットを用いるようにしても良い。なお、相互認証後の秘密通信においては、データは一時鍵K_{temp}で暗号化されるだけでなく、その暗号化された送信データに署名が付されることがある。

【０１９２】

署名の検証、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１９３】

図５３は、ユーザホームネットワーク５内の決済可能機器が、電子配信サービスセンタ１へ課金情報を送信するときの動作を説明する図である。ユーザホームネットワーク５内の決済可能機器は、登録情報から代理決済すべき対象機器を検索し、相互認証を行い、課金情報を共有した一時鍵K_{temp}（この鍵は、相互認証するたびに異なる）で暗号化して送らせる（このとき、データに署名が付いている）。全ての機器について処理が終わった後、電子配信サービスセンタ１と相互認証をし、共有した一時鍵で全ての課金情報を暗号化し、これらに署名データを付け、登録情報、必要に応じて取扱方針、価格情報と共に電子配信サービスセンタ１に送信する。なお、ユーザホームネットワーク５から電子配信サービスセンタ１へ送信される課金情報に、取扱方針のＩＤや価格情報のＩＤ等の金額の分配に必要な情報が含まれていることにより、情報量の多い取扱方針や価格情報は必ずしも送信する必要はない。ユーザ管理部１８はこれを受信する。ユーザ管理部１８は、受信した課金情報、登録情報、取扱方針、および価格情報に対する署名データの検証を行う。署名の検証は図１１で説明した方法と同じなため詳細は省略する。次に、ユーザ管理部１８は、相互認証のときに共有した一時鍵K_{temp}で

課金情報を復号化し、取扱方針、および価格情報と共に経歴データ管理部１５に送信する。

【０１９４】

因みに、この実施の形態においては、相互認証後に送信されるデータは必要に応じて一時鍵K_{temp}で暗号化される。例えばコンテンツ鍵K_{co}や配送鍵K_dは内容が見られてしまうとデータを不正に利用されてしまうため一時鍵K_{temp}で暗号化して外部から見えないようにする必要がある。これに対して課金情報や使用許諾条件情報等は内容が見られても、データを不正に利用することができないため、必ずしも一時鍵K_{temp}で暗号化する必要はないが、例えば課金情報の金額が改竄されたり使用許諾条件情報の使用条件が緩くなるように改竄されると金額の授受に関係する当事者に損害が発生することになる。従って、課金情報や使用許諾条件情報には署名を付して送信することにより改竄を防止している。ただし、コンテンツ鍵K_{co}や配送鍵K_dを送信する場合にも署名を付けても良い。

【０１９５】

そして、送信側では送られるデータに対して、又は送られるデータを一時鍵K_{temp}で暗号化したデータに対して署名を生成し、データ及び署名を送信する。受信側では、送られたデータが一時鍵K_{temp}で暗号化されていない場合には署名を検証することによりデータを得、又は送られたデータが一時鍵K_{temp}で暗号化されている場合には署名を検証した後に一時鍵K_{temp}でデータを復号することによりデータを得る。この実施の形態において、相互認証後に送信されるデータについては、以上の方法により署名及び必要に応じて一時鍵K_{temp}による暗号化が施される場合がある。

【０１９６】

ユーザ管理部１８は、鍵サーバ１４から配送鍵K_dを受信し、これを共有した一時鍵K_{temp}で暗号化して署名データを付加し、ユーザ登録データベースから登録情報を作成し、一時鍵K_{temp}で暗号化された配送鍵K_d、署名データ、登録情報をユーザホームネットワーク５内の決済可能機器に送信する。登録情報の作成方法については、図８で説明した通りでありここでの詳細説明は省略する。

【０１９７】

課金請求部１９は、決済を実行するとき、経歴データ管理部１５から課金情報、必要に応じて取扱方針、および価格情報を受信し、ユーザへの請求金額を算出し、請求情報を出納部２０に送信する。出納部２０は、銀行等と通信し、決済処理を実行する。その際、ユーザの未払い料金等の情報があれば、それらの情報は決済報告の形で課金請求部１９およびユーザ管理部１８に送信され、ユーザ登録データベースに反映され、以降のユーザ登録処理、または決済処理時に参照される。

【０１９８】

一時鍵K_{temp}で暗号化された配送鍵K_d、署名データ、登録情報を受信したユーザホームネットワーク５内の決済可能機器は、記憶してあった登録情報を更新すると共に、登録情報を検査し、登録がなされていれば、署名データを検証した後、配送鍵K_dを一時鍵K_{temp}で復号化し、暗号処理部内の記憶モジュールに記憶されている配送鍵K_dを更新し、記憶モジュール内の課金情報を削除する。続いて、登録情報から代理決済すべき対象機器を検索し、当該検索により見つかった機器ごとに相互認証を行い、暗号処理部の記憶モジュールから読み出した配送鍵K_dを検索により見つかった機器ことに異なる一時鍵K_{temp}で暗号化し、それぞれの機器ごとに署名を付け登録情報と共にそれぞれの機器に送信する。代理決済すべき対象機器が全て終わった時点で処理が終了する。

【０１９９】

これらのデータを受信した対象機器は、決済可能機器と同様に登録情報を検査し、署名データを検証した後、配送鍵K_dを一時鍵K_{temp}で復号化し、記憶モジュール内の配送鍵K_dを更新し、課金情報を削除する。

【０２００】

なお、登録情報の登録項目が「登録不可」となっていた機器については、課金が行われなかったため、配送鍵K_dの更新、課金情報の削除は行わない（登録項目の内容は、使用を含めて一切の停止、購入処理の停止、処理が正常に行われた状態等、記述されていない種々の場合があり得る）。

【０２０１】

図５４は電子配信サービスセンタ１の利益分配処理の動作を説明する図である。経歴データ管理部１５は、ユーザ管理部１８から送信された課金情報、必要に応じて取扱方針、および価格情報を保持・管理する。利益分配部１６は、経歴データ管理部１５から送信された課金情報、必要に応じて取扱方針および価格情報からコンテンツプロバイダ２、サービスプロバイダ３、および電子配信サービスセンタ１それぞれの利益を算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、および出納部２０に送信する。出納部２０は、銀行等と通信し、決済を行う。サービスプロバイダ管理部１１は、利益分配部１６から受信した分配情報をサービスプロバイダ２に送信する。コンテンツプロバイダ管理部１２は、利益分配部１６から受信した分配情報をコンテンツプロバイダ３に送信する。

【０２０２】

監査部２１は、経歴データ管理部１５から課金情報、取扱方針、および価格情報を受信し、データに矛盾がないか監査する。例えば、課金情報内の価格が価格情報のデータと一致しているかどうか、分配率が一致しているかどうか等を監査し、取扱方針と価格情報が矛盾していないかどうか監査する。また、監査部２１の処理としては、ユーザホームネットワーク５から入金された金額と、利益分配した合計金額又はサービスプロバイダ３へ送った金額との整合性を監査する処理や、ユーザホームネットワーク５の機器から供給された課金情報内のデータに例えば存在し得ないコンテンツプロバイダＩＤ、サービスプロバイダＩＤや考えられない取り分、価格等が含まれているか否かを監査する処理がある。

【０２０３】

図５５は、電子配信サービスセンタ１の、コンテンツの利用実績をＪＡＳＲＡＣに送信する処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの利用実績を示す課金情報を著作権管理部１３および利益分配部１６に送信する。利益分配部１６は、課金情報からＪＡＳＲＡＣに対する請求金額および支払金額を算出し、支払情報を出納部２０に送信する。出納部２０は、銀行等と通信し、決済処理を実行する。著作権管理部１３は、ユーザのコンテンツ

の利用実績をＪＡＳＲＡＣに送信する。

【０２０４】

次に、ＥＭＤシステムの処理について説明する。図５６は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップＳ４０において、電子配信サービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に個別鍵K_i、配送鍵K_dで暗号化された個別鍵K_iおよびコンテンツプロバイダ２の公開鍵証明書を送信し、コンテンツプロバイダ２がこれを受信する。その処理の詳細は、図５７のフローチャートを参照して後述する。ステップＳ４１において、ユーザは、ユーザホームネットワーク５の機器（例えば、図１５のホームサーバ５１）を操作し、ユーザホームネットワーク５の機器を電子配信サービスセンタ１のユーザ管理部１８に登録する。この登録処理の詳細は、図５９のフローチャートを参照して後述する。ステップＳ４２において、電子配信サービスセンタ１のユーザ管理部１８は、ユーザホームネットワーク５と、図５２について上述したように相互認証した後、ユーザホームネットワーク５の機器に、配送鍵K_dを送信する。ユーザホームネットワーク５はこの鍵を受信する。この処理の詳細は、図６２のフローチャートを参照して説明する。

【０２０５】

ステップＳ４３において、コンテンツプロバイダ２の署名生成部３８は、コンテンツプロバイダセキュアコンテナを生成し、それをサービスプロバイダ３に送信する。この処理の詳細は、図６５のフローチャートを参照して後述する。ステップＳ４４において、サービスプロバイダ３の署名生成部４５は、サービスプロバイダセキュアコンテナを生成し、それをユーザホームネットワーク５へ、ネットワーク４を介して送信する。この送信処理の詳細は、図６６のフローチャートを参照して後述する。ステップＳ４５において、ユーザホームネットワーク５の購入モジュール９４は、購入処理を実行する。購入処理の詳細は、図６７のフローチャートを参照して後述する。ステップＳ４６において、ユーザは、ユーザホームネットワーク５の機器でコンテンツを再生する。再生処理の詳細は、図７２のフローチャートを参照して後述する。

【０２０６】

図５７は、図５６のＳ４０に対応する、電子配信サービスセンタ１がコンテンツプロバイダ２へ個別鍵K_i、配送鍵K_dで暗号化された個別鍵K_iおよび公開鍵証明書を送信し、コンテンツプロバイダ２がこれを受信する処理の詳細を説明するフローチャートである。ステップＳ５０において、電子配信サービスセンタ１の相互認証部１７は、コンテンツプロバイダ２の相互認証部３９と相互認証する。この相互認証処理は、図５２で説明したので、その詳細は省略する。相互認証処理により、コンテンツプロバイダ２が正当なプロバイダであることが確認されたとき、ステップＳ５１において、コンテンツプロバイダ２は、電子配信サービスセンタ１のコンテンツプロバイダ管理部１２から送信された個別鍵K_i、配送鍵K_dで暗号化された個別鍵K_iおよび証明書を受信する。ステップＳ５２において、コンテンツプロバイダ２は受信した個別鍵K_iを耐タンパメモリ４０Ａに保存し、配送鍵K_dで暗号化された個別鍵K_iおよび証明書をメモリ４０Ｂに保存する。

【０２０７】

このように、コンテンツプロバイダ２は、電子配信サービスセンタ１から個別鍵K_i、配送鍵K_dで暗号化された個別鍵K_iおよび証明書を受け取る。同様に、図５６に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ２以外に、サービスプロバイダ３も、図５７と同様の処理で、電子配信サービスセンタ１から個別鍵K_i（コンテンツプロバイダ２の個別鍵K_iとは異なる）、配送鍵K_dで暗号化された個別鍵K_iおよび証明書を受け取る。

【０２０８】

なお、メモリ４０Ａは、コンテンツプロバイダ２が秘密裏に保持しなくてはならない個別鍵K_iを保持するため、第３者に容易にデータを読み出されない耐タンパメモリが望ましいが、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。また、メモリ４０Ｂは、配送鍵K_dで暗号化された個別鍵K_i、コンテンツプロバイダ２の証明書が保存されるだけであるため、通常の記憶装置等何でもよい（秘密にする必要がない）。また、メモリ４０Ａ、４０

Ｂを一つにしてもかまわない。

【０２０９】

図５８は、ホームサーバ５１が、電子配信サービスセンタ１のユーザ管理部１８に決済情報を登録する処理を説明するフローチャートである。ステップＳ６０において、ホームサーバ５１は、大容量記憶部６８に記憶されている公開鍵証明書を、暗号処理部６５の相互認証モジュール９５で、電子配信サービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図５２を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ６０で、ホームサーバ５１が電子配信サービスセンタ１のユーザ管理部１８に送信する証明書は、図３２に示すデータ（ユーザ機器の公開鍵証明書）を含む。

【０２１０】

ステップＳ６１において、ホームサーバは個人の決済情報（ユーザのクレジットカード番号や、決済機関の口座番号等）の登録が新規登録か否かを判定し、新規登録であると判定された場合、ステップＳ６２に進む。ステップＳ６２において、ユーザは入力手段６３を用いて個人の決済情報を入力する。これらのデータは、暗号化ユニット１１２で一時鍵K_{temp}を用いて暗号化され、通信部６１を介して電子配信サービスセンタ１のユーザ管理部１８に送信される。

【０２１１】

ステップＳ６３において、電子配信サービスセンタ１のユーザ管理部１８は、受信した証明書から機器のＩＤを取り出し、この機器のＩＤを基に、図７に示したユーザ登録データベースを検索する。ステップＳ６４において、電子配信サービスセンタ１のユーザ管理部１８は、受信したＩＤを有する機器の登録が可能であるか否かを判定し、受信したＩＤを有する機器の登録が可能であると判定された場合、ステップＳ６５に進み、受信したＩＤを有する機器が、新規登録であるか否かを判定する。ステップＳ６５において、受信したＩＤを有する機器が、新規登録であると判定された場合には、ステップＳ６６に進む。

【０２１２】

ステップＳ６６において、電子配信サービスセンタ１のユーザ管理部１８は、決済ＩＤを新規に発行すると共に、一時鍵で暗号化された決済情報を復号化し、

決済ＩＤおよび決済情報を、機器ＩＤ、決済ＩＤ、決済情報（口座番号やクレジットカード番号等）、取引停止情報等を記憶している決済情報データベースに機器のＩＤに対応させて登録し、決済ＩＤをユーザ登録データベースに登録する。ステップ６７において、ユーザ登録データベースに登録したデータに基づき登録情報を作成する。この登録情報は、図８で説明しているので、その詳細は省略する。

【０２１３】

ステップＳ６８において、電子配信サービスセンタ１のユーザ管理部１８は、作成した登録情報をホームサーバ５１に送信する。ステップＳ６９において、ホームサーバ５１の上位コントローラ６２は、受信した登録情報を大容量記憶部６８に保存する。

【０２１４】

ステップＳ６１において、決済情報の登録が更新登録であると判定された場合、手続きは、ステップＳ７０に進み、ユーザは入力手段６３を用いて個人の決済情報を入力する。これらのデータは、暗号化ユニット１１２で一時鍵K_{temp}を用いて暗号化され、既に決済登録時に発行された登録情報と共に通信部６１を介して電子配信サービスセンタ１のユーザ管理部１８に送信される。

【０２１５】

ステップＳ６４において、受信したＩＤを有する機器の登録が不可であると判定された場合、ステップＳ７１に進み、電子配信サービスセンタ１のユーザ管理部１８は、登録拒絶の登録情報を作成し、ステップＳ６８に進む。

【０２１６】

ステップＳ６５において、受信したＩＤを有する機器が、新規登録でないと判定された場合、手続きは、ステップＳ７２に進み、電子配信サービスセンタ１のユーザ管理部１８は、一時鍵で暗号化された決済情報を復号化し、機器のＩＤに対応させて決済情報登録データベースに更新登録し、ステップＳ６７に進む。

【０２１７】

このように、ホームサーバ５１は、電子配信サービスセンタ１に登録される。

【０２１８】

図５９は、登録情報に機器のＩＤを新規登録する処理を説明するフローチャートである。ステップＳ８０における相互認証処理は、図５２で説明した処理と同様なため、説明を省略する。ステップＳ８１において、図５８のステップＳ６３と同じであるためその説明は省略する。ステップＳ８２は、図５８のステップＳ６４と同じであるためその説明は省略する。ステップＳ８３において、電子配信サービスセンタ１のユーザ管理部１８は、ユーザ登録データベース内の機器ＩＤに対応する登録項目を「登録」に設定し、機器ＩＤを登録する。ステップＳ８４において、電子配信サービスセンタ１のユーザ管理部１８は、ユーザ登録データベースに基づき、図８に示すような登録情報を作成する。ステップＳ８５は、図５８のステップＳ６８と同じであるためその説明は省略する。ステップＳ８６は、図５８のステップＳ６９と同じであるためその説明は省略する。

【０２１９】

ステップＳ８２において、受信したＩＤを有する機器の登録が不可であると判定された場合、ステップＳ８７に進み、電子配信サービスセンタ１のユーザ管理部１８は、登録拒絶の登録情報を作成し、ステップＳ８５に進む。

【０２２０】

このように、ホームサーバ５１は、電子配信サービスセンタ１に登録される。

【０２２１】

図６０は、既に登録された機器を経由し、別の機器を追加登録する際の処理を説明するフローチャートである。ここでは、ホームサーバ５１が既に登録されており、そこに据置機器５２を登録する例で説明する。ステップＳ９０において、ホームサーバ５１は、据置機器５２と相互認証する。相互認証処理は、図５２で説明した処理と同様なため、説明を省略する。ステップＳ９１において、ホームサーバ５１は、電子配信サービスセンタ１と相互認証する。ステップＳ９２において、ホームサーバ５１は、大容量記憶部６８から読み出した登録情報、およびステップＳ９０で据置機器５２と相互認証した際に入手した据置機器５２の証明書を電子配信サービスセンタ１に送信する。ステップＳ９３は、図５９のステップＳ８１と同じであるためその説明は省略する。ステップＳ９４は、図５９のス

テップＳ８２と同じであるためその説明は省略する。ステップＳ９５は、図５９のステップＳ８３と同じであるためその説明は省略する。ステップＳ９６において、電子配信サービスセンタ１のユーザ管理部１８は、ホームサーバ５１から受信した登録情報に加え、据置機器５２の情報を追加した登録情報を新規に作成する。ステップＳ９７は、図５９のステップＳ８５と同じであるためその説明は省略する。ステップＳ９８は、図５９のステップＳ８６と同じであるためその説明は省略する。

【０２２２】

そして、ステップＳ９９Ａにおいてホームサーバ５１は受信した登録情報を据置機器５２に送信し、ステップＳ９９Ｂにおいて据置機器５２は受信した登録情報を小容量記憶部７５に保存する。

【０２２３】

ステップＳ９４において、受信したＩＤを有する機器の登録が不可であると判定された場合、ステップＳ９９に進み、電子配信サービスセンタ１のユーザ管理部１８は、据置機器５２のみ登録拒絶とした登録情報（従って、ホームサーバ５１は登録済みのまま）を作成し、ステップＳ９７に進む（ステップＳ９１でホームサーバ５１が電子配信サービスセンタ１と相互認証に成功しているということは、ホームサーバ５１が登録可であることを意味している）。

【０２２４】

かくして、据置機器５２は、図６０に示した処理手順により電子配信サービスセンタ１に追加登録される。

【０２２５】

ここで、登録済の機器が登録の更新（登録情報の更新）を行うタイミングについて説明する。図６１は登録情報の更新を行うか否かを種々の条件に基づいて判断する処理手順を示し、ステップＳ６００においてホームサーバ５１は配送鍵K_d、登録情報又は課金情報のすい上げから予め決められた一定期間が経過したか否かを時計（図示せず）及び判断部（図示せず）によって判断する。ここで肯定結果が得られると、このことは配送鍵K_d、登録情報又は課金情報のすい上げから一定の期間が経過していることを表しており、このときホームサーバ５１はス

テップＳ６０７に移って登録情報の更新処理を実行する。この処理については図６２において後述する。

【０２２６】

これに対してステップＳ６００において否定結果が得られると、このことは配送鍵K_d、登録情報又は課金情報のすい上げから一定の期間が経過していないこと、すなわち期間の経過について登録情報の更新条件を満たしていないことを表しており、このときホームサーバ５１はステップＳ６０１に移る。

【０２２７】

ステップＳ６０１においてホームサーバ５１は、コンテンツの購入回数が規定の回数に達しているか否かを判断する。ここで肯定結果が得られると、ホームサーバ５１はステップＳ６０７に移って登録情報更新処理を実行し、これに対してステップＳ６０１において否定結果が得られると、このことはコンテンツの購入回数について登録情報の更新条件を満たしていないことを表していることによりホームサーバ５１は続くステップＳ６０２に移る。

【０２２８】

ステップＳ６０２において、ホームサーバ５１は、コンテンツの購入金額が規定の金額に達しているか否かを判断する。ここで肯定結果が得れらると、ホームサーバ５１はステップＳ６０７に移って登録情報更新処理を実行し、これに対してステップＳ６０２において否定結果が得られると、このことはコンテンツの購入金額について登録情報の更新条件を満たしていないことを表していることによりホームサーバ５１は続くステップＳ６０３に移る。

【０２２９】

ステップＳ６０３において、ホームサーバ５１は、配送鍵K_dの有効期限が切れているか否かを判断する。配送鍵K_dの有効期限が切れているか否かを判断する方法としては、配信されたデータの配送鍵K_dのバージョンが記憶モジュール９２に保存されている３つのバージョンの配送鍵K_dのいずれかのバージョンと一致するか否か又は、最近の配送鍵K_dのバージョンより古いか否かを調べる。この比較結果が一致していない場合又は最近の配送鍵K_dのバージョンより古い場合には、記憶モジュール９２内の配送鍵K_dの有効期限が切れていることにな

り、ホームサーバ５１はステップＳ６０３において肯定結果を得ることによりステップＳ６０７に移って登録情報の更新処理を実行する。これに対してステップＳ６０３において否定結果が得られると、このことは配送鍵K_dの有効期限について登録情報の更新条件を満たしていないことを表しており、このときホームサーバ５１は続くステップＳ６０４に移る。

【０２３０】

ステップＳ６０４において、ホームサーバ５１は、当該ホームサーバ５１に他機器が新規接続されたか否か、又は接続されていた他機器が切り離されたか否かといったネットワーク構成の変更の有無を判断する。ここで肯定結果が得られると、このことはネットワーク構成に変更があったことを表しており、このときホームサーバ５１はステップＳ６０７に移って登録情報の更新処理を実行する。これに対してステップＳ６０４において否定結果が得られると、このことはネットワーク構成について登録情報の更新条件を満たしていないことを表しており、ホームサーバ５１は続くステップＳ６０５に移る。

【０２３１】

ステップＳ６０５において、ホームサーバ５１は、ユーザからの登録情報更新要求があったか否かを判断し、登録情報更新要求があった場合にはステップＳ６０７に移って登録情報の更新処理を実行し、登録情報更新要求がなかった場合にはステップＳ６０６に移る。

【０２３２】

ステップＳ６０６において、ホームサーバ５１は接続された他の機器について上述のステップＳ６００～ステップＳ６０５における更新判断を行い、更新すべき判断結果が得られたときステップＳ６０７に移って登録情報の更新処理を行い、これに対して更新すべき判断結果が得られないとき上述のステップＳ６００から同様の処理を繰り返す。これにより、ホームサーバ５１は登録情報の更新処理を行うタイミングを得ることができる。なお、ホームサーバ５１が他の機器の更新開始条件を調べるのではなく、他の機器が独自に調べて、自らホームサーバ５１に要求を出すようにしてもよい。

【０２３３】

図６２は、登録済みの機器が登録を更新（登録情報の更新）し、決済処理を行い、配送鍵K_dの再配布を受ける動作を説明するフローチャートである。ステップＳ１００における相互認証処理は、図５２で説明した処理と同様なため、説明を省略する。ステップＳ１０１において、ホームサーバ５１は、記憶モジュール９２に記憶されている課金情報を、暗号処理部９６の暗号化ユニット１１２で一時鍵K_{temp}を用いて暗号化し、署名生成ユニット１１４で署名を生成し、署名を付加する。そして、暗号化された課金情報及びその署名と、大容量記憶部６８に記憶されている取扱方針、価格情報および登録情報を合わせて電子配信サービスセンタ１に送信する。なお、このとき、取扱方針および価格情報はモデルによっては送信する必要がない。なぜなら、コンテンツプロバイダ２およびサービスプロバイダ３が予め電子配信サービスセンタ１に送信している場合があったり、課金情報に取扱方針、価格情報のうちの必要な情報が含まれている場合があるからである。

【０２３４】

ステップＳ１０２は、図５９のステップＳ８１と同じであるためその説明は省略する。ステップＳ１０３は、図５９のステップＳ８２と同じであるためその説明は省略する。ステップＳ１０４において、電子配信サービスセンタ１のユーザ管理部１８は署名検証ユニット１１５で署名を検証し、受信した課金情報を一時鍵K_{temp}で復号化し（受信データに電子署名がついている場合には、署名検証ユニット１１５で検証する）、（受信していれば）取扱方針および価格情報と共に経歴データ管理部１５に送信する。これを受信した経歴データ管理部１５は、受信データを保存・管理する。

【０２３５】

ステップＳ１０５において、電子配信サービスセンタ１のユーザ管理部１８は、ユーザ登録データベース内の機器ＩＤに対応する登録項目を検証すると共に、データを更新する。例えば、図示せぬ登録日付や課金状況等などのデータである。ステップＳ１０６は、図５９のステップＳ８４と同じであるためその説明は省略する。ステップＳ１０７において、電子配信サービスセンタ１のユーザ管理部

は、鍵サーバ１４から供給された配送鍵K_dを一時鍵K_{temp}で暗号化し、登録情報と共にホームサーバ５１に送信する。

【０２３６】

ステップＳ１０８において、ホームサーバ５１は受信した登録情報を大容量記憶部６８に保存する。ステップＳ１０９において、ホームサーバ５１は、受信した登録情報を暗号処理部６５に入力し、暗号処理部６５では、登録情報に含まれる電子署名を署名検証ユニット１１５で検証すると共に、ホームサーバ５１の機器ＩＤが登録されているか確認させ、検証に成功し、課金処理が完了したことを確認した際にはステップＳ１１０に進む。ステップＳ１１０において、ホームサーバ５１は、受信した配送鍵K_dを暗号処理部６５に入力する。暗号処理部６５では、受信した配送鍵K_dを暗号／復号化モジュール９６の復号化ユニット１１１で一時鍵K_{temp}を用いて復号化し、記憶モジュール９２に保存（更新）し、記憶モジュール９２に保持していた課金情報を消去する（これで、決済済みとなる）。

【０２３７】

ステップＳ１０３において、受信したＩＤを有する機器の登録が不可であると判定された場合、ステップＳ１１１に進み、電子配信サービスセンタ１のユーザ管理部１８は、登録拒絶とした登録情報を作成し、ステップＳ１１２に進む。ステップＳ１１２では、ステップＳ１０７と異なり、登録情報のみをホームサーバ５１に送信する。

【０２３８】

ステップＳ１０９において、登録情報に含まれる署名の検証に失敗するか、登録情報に含まれる「登録」の項目（例えば、課金処理失敗→購入処理ができない、登録拒否→再生等の処理を含め暗号処理部の機能の停止、取引一時停止→課金処理は成功したが、何らかの理由で購入を停止する、等が考えられる）に「登録可」が書かれていない場合は、ステップＳ１１３に進み所定のエラー処理を行う。

【０２３９】

このように、ホームサーバ５１は、登録情報を更新すると共に、課金情報を電

子配信サービスセンタ１に送信し、代わりに配送鍵K_dの供給を受ける。

【０２４０】

図６３及び図６４は、据置機器５２がホームサーバ５１を介して決済、登録情報の更新、配送鍵K_dの更新を行う処理を説明するフローチャートを示した図である。ステップＳ１２０において、ホームサーバ５１の相互認証モジュール９４と据置機器の図示せぬ相互認証モジュールは、相互認証を行う。相互認証処理は、図５２で説明した処理と同様なため、説明を省略する。なお、相互認証処理で説明したように、ホームサーバ５１と据置機器５２は互いに証明書を交換し合っているため、相手の機器ＩＤはわかっているものとする。ステップＳ１２１において、ホームサーバ５１の上位コントローラ６２は、大容量記憶部６８から登録情報を読み出し、暗号処理部６５に検査させる。上位コントローラ６２から登録情報を受け取った暗号処理部６５は、登録情報内の署名を検証し、据置機器のＩＤがあるかどうか判定し、登録情報に据置機器のＩＤがあった際にはステップＳ１２２に進む。

【０２４１】

ステップＳ１２２において、登録情報に据置機器５２のＩＤが登録されているか否かを判定し、据置機器５２のＩＤが登録されている場合には、ステップＳ１２３に進む。ステップＳ１２３において、据置機器５２の暗号処理部７３は、記憶モジュールに保存されている課金情報を読み出し、暗号化ユニットで一時鍵K_{temp}を用いて暗号化する。また、課金情報に対応する署名を、署名生成ユニットで生成する。署名の生成は図１０で説明したのでその詳細は省略する。一時鍵K_{temp}で暗号化された課金情報およびその署名を受け取った上位コントローラ７２は、必要に応じて課金情報に対応する取扱方針および価格情報を小容量記憶部７５から読み出し、一時鍵K_{temp}で暗号化された課金情報とその署名、必要に応じて課金情報に対応する取扱方針および価格情報をホームサーバ５１に送信する。

【０２４２】

これらのデータを受信したホームサーバ５１は、受信していれば取扱方針および価格情報を大容量記憶部６８に記憶すると共に、一時鍵K_{temp}で暗号化された課金情報およびその署名を暗号処理部６５に入力する。一時鍵K_{temp}で暗号化さ

れた課金情報およびその署名を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で、一時鍵K_{temp}で暗号化された課金情報に対する署名を検証する。署名の検証は図１１で説明したの処理と同じであるため、その詳細は省略する。そして、暗号／復号化モジュール９６の復号化ユニット１１１は、一時鍵K_{temp}で暗号化された課金情報を復号化する。

【０２４３】

ステップＳ１２４において、ホームサーバ５１は、電子配信サービスセンタ１の相互認証部１７と相互認証し一時鍵$K_{temp}2$を共有する。ステップＳ１２５において、ホームサーバ５１は、据置機器５２から送られたきた課金情報を暗号／復号化モジュール９６の暗号化ユニット１１２で一時鍵$K_{temp}2$を用いて暗号化する。このとき、ホームサーバ５１の課金情報を合わせて暗号化しておいてもよい。また、一時鍵$K_{temp}2$で暗号化された課金情報に対応する署名を、暗号／復号化モジュール９６の署名生成ユニット１１４で生成する。一時鍵$K_{temp}2$で暗号化された課金情報、およびその署名を受け取った上位コントローラ６２は、必要に応じて課金情報に対応する取扱方針、価格情報、および登録情報を大容量記憶部６８から読み出し、一時鍵$K_{temp}2$で暗号化された課金情報、その署名、必要に応じて課金情報に対応する取扱方針、価格情報および登録情報を電子配信サービスセンタ１のユーザ管理部１８に送信する。

【０２４４】

ステップＳ１２６において、電子配信サービスセンタ１のユーザ管理部１８は、ユーザ登録データベースを検索する。ステップＳ１２７において、ホームサーバ５１および据置機器５２がユーザ登録データベース内の「登録」の項目に、登録可で登録されているか否か判定し、登録されていると判定されていた場合、ステップＳ１２８に進む。ステップＳ１２８において、電子配信サービスセンタ１のユーザ管理部１８は、一時鍵$K_{temp}2$で暗号化された課金情報に対する署名を検証し、課金情報を一時鍵$K_{temp}2$で復号化する。そして、課金情報、受信してければ取扱方針および価格情報を経歴データ管理部１５に送信する。課金情報、受信していれば取扱方針および価格情報を受信した経歴データ管理部１５は、そのデータを管理・保存する。

【０２４５】

ステップＳ１２９において、電子配信サービスセンタ１のユーザ管理部１８は、ユーザ登録データベースを更新する（図示せぬ課金データ受信日時、登録情報発行日時、配送鍵交付日時等）。ステップＳ１３０において、電子配信サービスセンタ１のユーザ管理部１８は、登録情報を作成する（例えば図８の例）。ステップＳ１３１において、電子配信サービスセンタ１のユーザ管理部１８は、電子配信サービスセンタ１の鍵サーバ１４から受信した配送鍵K_dを一時鍵$K_{temp}2$で暗号化し、一時鍵$K_{temp}2$で暗号化された配送鍵K_dに対する署名を生成する。そして、登録情報、一時鍵$K_{temp}2$で暗号化された配送鍵K_dおよび一時鍵$K_{temp}2$で暗号化された配送鍵K_dに対する署名をホームサーバ５１に送信する。

【０２４６】

ステップＳ１３２において、ホームサーバ５１は、登録情報、一時鍵$K_{temp}2$で暗号化された配送鍵K_dおよび一時鍵$K_{temp}2$で暗号化された配送鍵K_dに対する署名を受信する。ホームサーバ５１の上位コントローラ６２は、一時鍵$K_{temp}2$で暗号化された配送鍵K_dおよび一時鍵$K_{temp}2$で暗号化された配送鍵K_dに対する署名を暗号処理部６５に入力する。暗号処理部６５において、暗号／復号化モジュール９６の署名検証ユニット１１５は、一時鍵$K_{temp}2$で暗号化された配送鍵K_dに対する署名を検証し、暗号／復号化モジュール９６の復号化ユニット１１１は、一時鍵$K_{temp}2$を用いて配送鍵K_dを復号化し、暗号／復号化モジュール９６の暗号化ユニット１１２は、復号化された配送鍵K_dを、据置機器５２との間で共有した一時鍵K_{temp}を用いて再暗号化する。最後に、暗号／復号化モジュール９６の署名生成ユニット１１４は、一時鍵K_{temp}を用いて暗号化された配送鍵K_dに対応する署名を生成し、一時鍵K_{temp}で暗号化された配送鍵K_dおよび一時鍵K_{temp}で暗号化された配送鍵K_dに対する署名を上位コントローラ６２に返送する。一時鍵K_{temp}で暗号化された配送鍵K_dおよび一時鍵K_{temp}で暗号化された配送鍵K_dに対する署名を受信した上位コントローラ６２は、電子配信サービスセンタ１から送られた来た登録情報と共に据置機器５２に送信する。

【０２４７】

ステップＳ１３３において、据置機器５２の上位コントローラ７２は、受信した登録情報を小容量記憶部７５に上書き保存する。ステップＳ１３４において、据置機器５２の暗号処理部７３は、受信した登録情報の署名を検証し、据置機器５２のＩＤの「登録」に対する項目が「登録可」になっているか否かを判定し、「登録可」になっていた場合には、ステップＳ１３５に進む。ステップＳ１３５において、据置機器５２の上位コントローラは、一時鍵K_{temp}で暗号化された配送鍵K_dおよび一時鍵K_{temp}で暗号化された配送鍵K_dに対する署名を暗号処理部７３に入力する。暗号処理部７３は、一時鍵K_{temp}で暗号化された配送鍵K_dに対する署名を検証し、一時鍵K_{temp}を用いて配送鍵K_dを復号化し、暗号処理部７３の記憶モジュール内の配送鍵K_dを更新すると共に、課金情報を消去する（なお、実際には消去せず、決済済みのマークを付けるだけの場合がある）。

【０２４８】

ステップＳ１２１において、据置機器５２のＩＤが登録情報に含まれていなかった場合、ステップＳ１３６に進み、図６０で説明した登録情報追加処理を開始し、ステップＳ１２３へと進む。

【０２４９】

ステップＳ１２７において、ユーザ登録データベース内の「登録」項目に対し、ホームサーバ５１のＩＤまたは据置機器５２のＩＤが「登録可」になっていなかった場合、ステップＳ１３７に進む。ステップＳ１３７は、ステップＳ１３０の場合と同様なため、その詳細は省略する。ステップＳ１３８は、ステップＳ１３１において、電子配信サービスセンタ１のユーザ管理部１８は、登録情報をホームサーバ５１に送信する。ステップＳ１３９において、ホームサーバ５１は、登録情報を据置機器５２に送信する。

【０２５０】

ステップＳ１２２において、登録情報における据置機器５２のＩＤに対する「登録」項目が、「登録可」になっていなかった場合、ステップＳ１３４において、登録情報における据置機器５２のＩＤに対する「登録」項目が、「登録可」になっていなかった場合、処理は終了する。

【０２５１】

なお、本方式による代理処理は、据置機器５２のみの処理になっているが、ホームサーバ５１につながる全ての機器やホームサーバ５１自身の課金情報を全て集め、一括処理しても良い。そして、全ての機器の登録情報、配送鍵K_dの更新を行う（本実施例において、受け取った登録情報、配送鍵K_dは、ホームサーバ５１で全くチェックされていない。ホームサーバ５１自身の処理も一括して行う場合には、当然チェックし、更新すべきである）。

【０２５２】

次に、図５６のステップＳ４３に対応する、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を、図６５のフローチャートを用いて説明する。ステップＳ１４０において、コンテンツプロバイダ２の電子透かし付加部３２は、コンテンツサーバ３１から読み出したコンテンツに、コンテンツプロバイダ２を示す所定のデータ、例えばコンテンツプロバイダＩＤなどを電子透かしの形で挿入し、圧縮部３３に供給する。ステップＳ１４１において、コンテンツプロバイダ２の圧縮部３３は、電子透かしが挿入されたコンテンツをＡＴＲＡＣ等の所定の方式で圧縮し、コンテンツ暗号部３４に供給する。ステップＳ１４２において、コンテンツ鍵生成部３５は、コンテンツ鍵K_{co}として用いる鍵を生成させ、コンテンツ暗号部３４およびコンテンツ鍵暗号部３６に供給する。ステップＳ１４３において、コンテンツプロバイダ２のコンテンツ暗号部３４は、ＤＥＳなどの所定の方式で、コンテンツ鍵K_{co}を使用して、電子透かしが挿入され、圧縮されたコンテンツを暗号化する。

【０２５３】

ステップＳ１４４において、コンテンツ鍵暗号部３６は、ＤＥＳなどの所定の方法で、図５６のステップＳ４０の処理により、電子配信サービスセンタ１から供給されている個別鍵K_iでコンテンツ鍵K_{co}を暗号化する。ステップＳ１４５において、取扱方針生成部３７は、コンテンツの取り扱い方針を規定し、図３３又は図３４に示すような取扱方針を生成する。ステップＳ１４６において、コンテンツプロバイダ２の署名生成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、暗号化された個別鍵K_iおよび取扱方針生成部３７から供

給された取扱方針に対し署名を生成する。署名の生成は図１０を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１４７において、コンテンツプロバイダ２は、暗号化されたコンテンツおよびその署名、暗号化されたコンテンツ鍵K_{co}およびその署名、暗号化された個別鍵K_iおよびその署名、取扱方針およびその署名（以降、これら４つの署名付きデータをコンテンツプロバイダセキュアコンテナと呼ぶ）、予め認証局からもらっておいたコンテンツプロバイダ２の証明書を、図示せぬ送信部を用いてサービスプロバイダ３に送信する。

【０２５４】

以上のように、コンテンツプロバイダ２は、サービスプロバイダ３に、コンテンツプロバイダセキュアコンテナを送信する。

【０２５５】

次に、図５６のステップＳ４４に対応する、サービスプロバイダ３がホームサーバ５１にサービスプロバイダセキュアコンテナを送信する処理を、図６６のフローチャートを用いて説明する。なお、サービスプロバイダ３は、コンテンツプロバイダ２から送信されたデータをコンテンツサーバ４１に予め保存しているものとして説明する。ステップＳ１５０において、サービスプロバイダ３の証明書検証部４２は、コンテンツサーバ４１からコンテンツプロバイダ２の証明書の署名を読み出し、証明書内の署名を検証する。署名の検証は図１１を参照して説明した方法と同様なため、その詳細は省略する。証明書に改竄がなければ、コンテンツプロバイダ２の公開鍵K_{pcp}を取り出す。

【０２５６】

ステップＳ１５１において、サービスプロバイダ３の署名検証部４３は、コンテンツプロバイダ２の送信部から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２の公開鍵K_{pcp}で検証する（取扱方針の署名のみ検証する場合がある）。署名の検証に失敗し、改竄が発見された場合は、処理を終了する。なお、署名の検証は図１１を参照して説明した方法と同様なため、その詳細は省略する。

【０２５７】

コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップＳ１５２において、サービスプロバイダ３の値付け部４４は、取扱方針を基に、図３７や図３８で説明した価格情報を作成する。ステップＳ１５３において、サービスプロバイダ３の署名生成部４５は、価格情報に対する署名を生成し、コンテンツプロバイダセキュアコンテナ、価格情報、および価格情報の署名を合わせサービスプロバイダセキュアコンテナを作成する。

【０２５８】

ステップＳ１５４において、サービスプロバイダ３の図示せぬ送信部は、ホームサーバ５１の通信部６１に、サービスプロバイダ３の証明書、コンテンツプロバイダ２の証明書およびサービスプロバイダセキュアコンテナを送信し、処理を終了する。

【０２５９】

このように、サービスプロバイダ３は、ホームサーバ５１にサービスプロバイダセキュアコンテナを送信する。

【０２６０】

図５６のステップＳ４５に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、ホームサーバ５１の購入処理の詳細を、図６７のフローチャートを用いて説明する。ステップＳ１６１において、ホームサーバ５１は図６１及び図６２について上述した登録情報更新処理を実行した後、ステップＳ１６２において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した登録情報をホームサーバ５１の暗号処理部６５に入力する。登録情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で登録情報の署名を検証した後、ホームサーバ５１のＩＤに対する「購入処理」の項目が「購入可」になっているか判定すると共に登録の項目を「登録可」になっていることを検査し、「購入可」及び「登録可」であった場合にはステップＳ１６３に進む。なお、署名検証、「登録可」、「購入可」の検査は登録情報検査モジュール９３で行うようにしても良い。ステップＳ１６３において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ

５１の大容量記憶部６８から読み出したコンテンツプロバイダ２の公開鍵証明書をホームサーバ５１の暗号処理部６５に入力する。

【０２６１】

コンテンツプロバイダ２の公開鍵証明書を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でコンテンツプロバイダ２の証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ２の公開鍵を取り出す。署名の検証の結果、改竄がなされていないことが確認された場合には、ステップＳ１６４に進む。ステップＳ１６４において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出したコンテンツをホームサーバ５１の暗号処理部６５に入力する。コンテンツを受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でコンテンツの署名を検証し、改竄がなされていないことが確認された場合には、ステップＳ１６５に進む。ステップＳ１６５において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出したコンテンツ鍵K_{co}をホームサーバ５１の暗号処理部６５に入力する。

【０２６２】

コンテンツ鍵K_{co}を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でコンテンツ鍵K_{co}の署名を検証し、改竄がなされていないことが確認された場合には、ステップＳ１６６に進む。ステップＳ１６６において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した個別鍵K_iをホームサーバ５１の暗号処理部６５に入力する。個別鍵K_iを受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で個別鍵K_iの署名を検証し、改竄がなされていないことが確認された場合には、ステップＳ１６７に進む。

【０２６３】

ステップＳ１６７において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した取扱方針をホームサーバ５１の暗号処理部６５に入力する。取扱方針を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で取扱方針の署名を検証し、改竄

がなされていないことが確認された場合には、ステップＳ１６８に進む。ステップＳ１６８において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出したサービスプロバイダ３の公開鍵証明書をホームサーバ５１の暗号処理部６５に入力する。

【０２６４】

サービスプロバイダ３の公開鍵証明書を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でサービスプロバイダ３の証明書の署名を検証した後、公開鍵証明書からサービスプロバイダ３の公開鍵を取り出す。署名の検証の結果、改竄がなされていないことが確認された場合には、ステップＳ１６９に進む。ステップＳ１６９において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した価格情報をホームサーバ５１の暗号処理部６５に入力する。価格情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で価格情報の署名を検証し、改竄がなされていないことが確認された場合には、ステップＳ１７０に進む。

【０２６５】

ステップＳ１７０において、ホームサーバ５１の上位コントローラ６２は、表示手段６４を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段６３を用いて購入項目を選択する。入力手段６３から入力された信号はホームサーバ５１の上位コントローラ６２に送信され、上位コントローラ６２は、その信号に基づいて購入コマンドを生成し、購入コマンドをホームサーバ５１の暗号処理部６５に入力する。なお、これらの入力処理は購入処理スタート時に行っても良い。これを受信した暗号処理部６５は、ステップＳ１６７で入力された取扱方針およびステップＳ１６９で入力された価格情報から課金情報および使用許諾条件情報を生成する。課金情報については、図４２で説明したので、その詳細は省略する。使用許諾条件情報については、図４１で説明したので、その詳細は省略する。

【０２６６】

ステップＳ１７１において、暗号処理部６５の制御部９１は、ステップＳ１７

０で生成した課金情報を記憶モジュール９２に保存する。ステップＳ１７２において、暗号処理部６５の制御部９１は、ステップＳ１７０で生成した使用許諾条件情報を暗号処理部６５の外部メモリ制御部９７に送信する。使用許諾条件情報を受信した外部メモリ制御部９７は、外部メモリ６７の改竄チェックを行った後、使用許諾条件情報を外部メモリ６７に書き込む。書き込む際の改竄チェックについては、図６９を用いて後述する。ステップＳ１７３において、暗号処理部６５の制御部９１は、ステップＳ１６６で入力された個別鍵K_iを、暗号／復号化モジュール９６の復号化ユニット１１１で、記憶モジュール９２から供給された配送鍵K_dを用いて復号化する。次に、暗号処理部６５の制御部９１は、ステップＳ１６５で入力されたコンテンツ鍵K_{co}を、暗号／復号化モジュール９６の復号化ユニット１１１で、先ほど復号化した個別鍵K_iを用いて復号化する。最後に、暗号処理部６５の制御部９１は、暗号／復号化モジュール９６の暗号化ユニット１１２で、記憶モジュール９２から供給された保存鍵K_{save}を用いてコンテンツ鍵K_{co}を暗号化する。ステップＳ１７４において、保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}は、暗号処理部６５の外部メモリ制御部９７を経由して外部メモリ６７に保存される。

【０２６７】

ステップＳ１６２でホームサーバ５１が購入処理できない機器であると判定された場合、又はステップＳ１６３でコンテンツプロバイダ２の公開鍵証明書の署名が正しくないと判定された場合、又はステップＳ１６４でコンテンツ鍵K_{co}で暗号化されたコンテンツの署名が正しくないと判定された場合、又はステップＳ１６５で個別鍵K_iで暗号化されたコンテンツ鍵K_{co}の署名が正しくないと判定された場合、又はステップＳ１６６で配送鍵K_dで暗号化された個別鍵K_iの署名が正しくないと判定された場合、又はステップＳ１６７で取扱方針の署名が正しくないと判定された場合、又はステップＳ１６８でサービスプロバイダ３の証明書の署名が正しくないと判定された場合、又はステップＳ１６９で価格情報の署名が正しくないと判定された場合、ホームサーバ５１はステップＳ１７６に進み、エラー処理を行う。なおステップＳ１６５、およびステップＳ１６６の処理をまとめ、コンテンツ鍵K_{co}、個別鍵K_iに対する唯一の署名を検証するように

してもよい。

【０２６８】

以上のように、ホームサーバ５１は、課金情報を記憶モジュール９２に記憶すると共に、コンテンツ鍵K_{co}を個別鍵K_iで復号化した後、コンテンツ鍵K_{co}を保存鍵K_{save}で暗号化し、外部メモリ６７に記憶させる。

【０２６９】

据置機器５２も、同様の処理で、課金情報を暗号処理部７３の記憶モジュールに記憶すると共に、コンテンツ鍵K_{co}を個別鍵K_iで復号化し、コンテンツ鍵K_{co}を保存鍵$K_{save}2$（ホームサーバ５１の鍵と異なる）で暗号化し、外部メモリ７９に記憶させる。

【０２７０】

図６８は、暗号処理部６５の外部メモリ制御部９７が、外部メモリ６７からデータを読み出す際に行う、改竄チェックの方法を説明するフローチャートである。図６８のステップＳ１８０において、暗号処理部６５の外部メモリ制御部９７は、外部メモリ６７から読み出すデータの場所を検索する（例えば図１６のブロック目の１番目のデータ）。ステップＳ１８１において、暗号処理部６５の外部メモリ制御部９７は、外部メモリ６７内の読み出し予定データを含む同一ブロック内全てのデータに対するハッシュ値（図１６の１ブロック目全体のハッシュ値）を計算する。このとき、読み出し予定のデータ（例えばコンテンツ鍵１と使用許諾条件情報１）以外は、ハッシュ値計算に使用後、破棄される。ステップＳ１８２において、ステップＳ１８１で計算したハッシュ値と暗号処理部６５の記憶モジュール９２に記憶されているハッシュ値（ICV_1）を比較する。一致していた場合、ステップＳ１８１で読み出しておいたデータを、外部メモリ制御部９７を介して制御部９１に送信し、一致していなかった場合、外部メモリ制御部９７はＳ１８３に移り、当該メモリブロックは改竄されているものとして以降の読み書きを禁止する（不良ブロックとする）。例えば、外部メモリを４ＭＢのフラッシュメモリとしたとき、このメモリを６４のブロックに分けたものと仮定する。従って、記憶モジュールには６４個のハッシュ値が記憶されている。データの読み出しを行う場合は、まず、データがある場所を検索し、そのデータを含む同

一ブロック内の全てのデータに対するハッシュ値を計算する。このハッシュ値が、記憶モジュール内の当該ロックに対応したハッシュ値と一致しているか否かで改竄をチェックする（図１６参照）。

【０２７１】

このように、暗号処理部６５の外部メモリ制御部９７は、外部メモリ６７の改竄チェックを行い、データを読み出す。

【０２７２】

図６９は、暗号処理部６５の外部メモリ制御部９７が、外部メモリ６７にデータを書き込む際に行う、改竄チェックの方法を説明するフローチャートである。図６９のステップＳ１９０Ａにおいて、暗号処理部６５の外部メモリ制御部９７は、外部メモリ６７にデータを書き込むことができる場所を検索する。ステップＳ１９１Ａにおいて、暗号処理部６５の外部メモリ制御部９７は、外部メモリ６７内に空きエリアがあるか否か判定し、空きエリアがあると判定した場合、ステップＳ１９２Ａに進む。ステップＳ１９２Ａにおいて、暗号処理部６５の外部メモリ制御部９７は、書き込み予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップＳ１９３Ａにおいて、ステップＳ１９２Ａで計算したハッシュ値と暗号処理部６５の記憶モジュール９２に記憶されているハッシュ値を比較し、一致していた場合、ステップＳ１９４Ａに進む。ステップＳ１９４Ａにおいて、書き込み予定領域にデータを書き込む。ステップＳ１９５Ａにおいて、暗号処理部６５の外部メモリ制御部９７は、書き込んだデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップＳ１９６Ａにおいて、制御部９１は、暗号処理部６５の記憶モジュール９２内のハッシュ値をステップＳ１９５Ａで計算したハッシュ値に更新する。

【０２７３】

ステップＳ１９３Ａにおいて、計算したハッシュ値が記憶モジュール９２内のハッシュ値と異なっていた場合、制御部９１は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値を不良ブロックを示す値に変更する）、ステップＳ１９０Ａへ進む。

【０２７４】

ステップＳ１９１Ａにおいて、外部メモリ６７に空きエリアがないと判定された場合、ステップＳ１９８Ａに進み、ステップＳ１９８Ａにおいて、外部メモリ制御部９７は、書き込みエラーを制御部９１に返送し、処理を終了する。

【０２７５】

外部メモリ制御部９７の外部メモリ６７への書き換え（更新）方法は、図７０に示すように、ステップＳ１９０Ｂにおいて暗号処理部６５の外部メモリ制御部９７は、外部メモリ６７のデータを書き換える場所を検索する。ステップＳ１９２Ｂにおいて、暗号処理部６５の外部メモリ制御部９７は、書き換え予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップＳ１９３Ｂにおいて、ステップＳ１９２Ｂで計算したハッシュ値と暗号処理部６５の記憶モジュール９２に記憶されているハッシュ値を比較し、一致していた場合、ステップＳ１９４Ｂに進む。ステップＳ１９４Ｂにおいて、書き換え予定領域のデータを書き換える。ステップＳ１９５Ｂにおいて、暗号処理部６５の外部メモリ制御部９７は、書き込んだデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップＳ１９６Ｂにおいて、制御部９１は、暗号処理部６５の記憶モジュール９２内のハッシュ値をステップＳ１９５Ｂで計算したハッシュ値に更新する。

【０２７６】

ステップＳ１９３Ｂにおいて、計算したハッシュ値が記憶モジュール９２内のハッシュ値と異なっていた場合、制御部９１は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値とを不良ブロックを示す値に変更する）、書き換え失敗とする。

【０２７７】

外部メモリ７９のデータの削除方法について、図７１を用いて説明する。ステップＳ１９０Ｃにおいて、暗号処理部７３の外部メモリ制御部は、外部メモリ７９のデータを削除する場所を検索する。ステップＳ１９２Ｃにおいて、暗号処理部７３の外部メモリ制御部は、データ削除予定データブロック内の、全てのデータに対するハッシュ値とを計算する。ステップＳ１９３Ｃにおいて、ステップＳ

１９２Ｃで計算したハッシュ値と暗号処理部７３の記憶モジュール（図示せず）に記憶されているハッシュ値を比較し、一致していた場合、ステップＳ１９４Ｃに進む。ステップＳ１９４Ｃにおいて、削除予定領域の削除予定であるデータを削除する。ステップＳ１９５Ｃにおいて、暗号処理部７３の外部メモリ制御部は、削除予定データを削除したデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップＳ１９６Ｃにおいて、暗号処理部７３は記憶モジュール内のハッシュ値をステップＳ１９５Ｃで計算したハッシュ値に更新する。

【０２７８】

ステップＳ１９３Ｃにおいて、計算したハッシュ値が記憶モジュール内のハッシュ値と異なっていた場合、暗号処理部７３は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値とを不良ブロックを示す値に変更する）、消去失敗とする。

【０２７９】

図５６のステップＳ４６に対応するホームサーバ５１がコンテンツを再生する処理の詳細を、図７２及び図７３のフローチャートを用いて説明する。ステップＳ２００において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の入力手段６３から再生指示されたコンテンツに対応するＩＤを、ホームサーバ５１の暗号処理部６５に入力する。ステップＳ２０１において、再生するコンテンツＩＤを受信した暗号処理部６５の制御部９１は、コンテンツＩＤを暗号処理部６５の外部メモリ制御部９７に送信し、コンテンツＩＤに対応するコンテンツ鍵K_{co}および使用許諾条件情報を検索させる。このとき、使用許諾条件情報が再生可能な権利であることを確認する。ステップＳ２０２において、暗号処理部６５の外部メモリ制御部９７は、コンテンツ鍵K_{co}および使用許諾条件情報を含むデータブロックのハッシュ値を計算し、暗号処理部６５の制御部９１に送信する。ステップＳ２０３において、暗号処理部６５の制御部９１は、暗号処理部６５の記憶モジュール９２に記憶されているハッシュ値とステップＳ２０２で受信したハッシュ値が一致しているか否か判定し、一致していた場合にはステップＳ２０４に進む。

【０２８０】

ステップＳ２０４において、暗号処理部６５の制御部９１は、使用許諾条件情報を必要に応じて更新する。例えば、使用許諾条件情報内の利用権が回数券であった場合、その回数を減算するなどの処理である。従って、更新する必要のない買い切りの権利などは、更新する必要がなく、その場合、ステップＳ２０８へジャンプする（図示していない）。ステップＳ２０５において、外部メモリ制御部９７は、制御部９１から送信された更新された使用許諾条件情報を、外部メモリ６７に書き換え更新する。ステップＳ２０６において、外部制御部９７は、書き換えたデータブロック内の全データに対するハッシュ値を計算し直し、暗号処理部６５の制御部９１に送信する。ステップＳ２０７において、暗号処理部６５の制御部９１は、暗号処理部６５の記憶モジュール９２に記憶されているハッシュ値を、ステップＳ２０６で算出したハッシュ値に書き換える。

【０２８１】

ステップＳ２０８において、暗号処理部６５と伸張部６６は相互認証を行い、一時鍵K_{temp}を共有する。相互認証処理は、図５１を用いて説明したのでその詳細は省略する。ステップＳ２０９において、暗号／復号化モジュール９６の復号化ユニット１１１は、外部メモリ９７から読み出したコンテンツ鍵K_{co}を、記憶モジュール９２から供給された保存鍵K_{save}で復号化する。ステップＳ２１０において、暗号／復号化モジュール９６の暗号化ユニット１１２は、先ほど伸張部６６と共有した一時鍵K_{temp}でコンテンツ鍵K_{co}を再暗号化する。ステップＳ２１１において、暗号処理部６５の制御部９１は、上位コントローラ６２を介して、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}を伸張部６６に送信する。

【０２８２】

ステップＳ２１２において、伸張部６６の鍵復号モジュール１０２は、相互認証モジュール１０１から供給された一時鍵K_{temp}でコンテンツ鍵K_{co}を復号化する。ステップＳ２１３において、上位コントローラ６２は大容量記憶部６８からコンテンツを読み出し、伸張部６６に供給する。コンテンツを受信した伸張部６６の復号モジュール１０３は、鍵復号モジュール１０２から供給されたコンテンツ鍵K_{co}を用いてコンテンツを復号化する。ステップＳ２１４において、伸張部

６６の伸張モジュール１０４は、コンテンツを所定の方式、例えばＡＴＲＡＣなどの方式により伸張する。ステップＳ２１５において、電子透かし付加モジュール１０５は、暗号処理部６５から指示されたデータを電子透かしの形でコンテンツに挿入する（暗号処理部から伸張部へ渡されるデータは、コンテンツ鍵K_{co}だけではなく、再生条件（アナログ出力、ディジタル出力、コピー制御信号付き出力（SCMS））、コンテンツ利用権を購入した機器ＩＤなども含まれている。挿入するデータは、このコンテンツ利用権を購入した機器のＩＤ（つまりは、使用許諾条件情報内の機器ＩＤ）などである）。ステップＳ２１６において、伸張部６６は、図示せぬスピーカを介して音楽を再生する。

【０２８３】

このように、ホームサーバ５１は、コンテンツを再生する。

【０２８４】

図７４は、ホームサーバ５１が据置機器５２のために、コンテンツ利用権を代理購入する処理の詳細を説明したフローチャートである。ステップＳ２２０において、ホームサーバ５１と据置機器５２は、相互認証する。相互認証処理は、図５２で説明した処理と同様なため、説明を省略する。ステップＳ２２１において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した登録情報を、ホームサーバ５１の暗号処理部６５に検査させる。上位コントローラ６２から登録情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５に、登録情報に付加されている署名を、暗号処理部６５の記憶モジュール９２から供給された電子配信サービスセンタ１の公開鍵で検証させる。署名の検証に成功した後、暗号処理部６５の制御部９１は、登録情報に据置機器のＩＤが登録され、「登録」及び「購入」の項目が「登録可」及び「購入化」になっているか判定し、「登録可」になっていると判定された場合にはステップＳ２２２に進む（なお、据置機器５２側でも登録情報を検査し、ホームサーバ５１が「登録可」になっていることを判定している）。ステップＳ２２５からステップＳ２２７は、図６７のステップＳ１６０からステップＳ１７１までと同様な処理なため、その詳細は省略する。

【０２８５】

ステップＳ２２８において、暗号処理部６５の制御部９１は、ステップＳ２２５で入力された配送鍵K_dで暗号化された個別鍵K_iを、暗号／復号化モジュール９６の復号化ユニット１１１で、記憶モジュール９２から供給された配送鍵K_dを用いて復号化する。次に、暗号処理部６５の制御部９１は、ステップＳ２２５で入力された個別鍵K_iで暗号化されたコンテンツ鍵K_{co}を、暗号／復号化モジュール９６の復号化ユニット１１１で、個別鍵K_iを用いて復号化する。そして、暗号処理部６５の制御部９１は、暗号／復号化モジュール９６の暗号化ユニット１１２で、ステップＳ２２０の相互認証時に据置機器５２と共有した一時鍵K_{temp}を用いてコンテンツ鍵K_{co}を再暗号化する。ステップＳ２２９において、暗号処理部６５の制御部９１は、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}と、ステップＳ２２６で生成した使用許諾条件情報に対し、暗号／復号化モジュール９６の署名生成ユニット１１４を用いて署名を生成し、上位コントローラ６２に送信する。一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}、使用許諾条件情報およびそれらの署名を受信したホームサーバ５１の上位コントローラ６２は、大容量記憶部６８からコンテンツ鍵K_{co}で暗号化されたコンテンツ（署名を含む。以下同じ）を読み出し、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}、使用許諾条件情報、それらの署名およびコンテンツ鍵K_{co}で暗号化されたコンテンツを据置機器５２に送信する。

【０２８６】

ステップＳ２３０において、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}、使用許諾条件情報、それらの署名およびコンテンツ鍵K_{co}で暗号化されたコンテンツを受信した据置機器５２は、署名を検証した後コンテンツ鍵K_{co}で暗号化されたコンテンツを据置機器５２の記録再生部７６に出力する。コンテンツ鍵K_{co}で暗号化されたコンテンツを受信した据置機器５２の記録再生部７６は、コンテンツ鍵K_{co}で暗号化されたコンテンツを記録メディア８０に保存する。

【０２８７】

ステップＳ２３１において、据置機器５２の暗号処理部７３は、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}を、暗号／復号化モジュールの復号化ユニット

で、ステップＳ２２０の相互認証時にホームサーバ５１と共有した一時鍵K_{temp}を用いて復号化する。そして、暗号処理部７３の制御部は、暗号／復号化モジュールの暗号化ユニットで、暗号処理部７３の記憶モジュールから供給された保存鍵$K_{save}2$を用いてコンテンツ鍵K_{co}を再暗号化する。

【０２８８】

ステップＳ２３２において、据置機器５２の暗号処理部７３は、保存鍵K_{save}２で暗号化されたコンテンツ鍵K_{co}とステップＳ２３０で受信した使用許諾条件情報を暗号処理部７３の外部メモリ制御部に送信し、外部メモリ７９に保存させる。外部メモリ制御部が外部メモリにデータを書き込む処理については、図６９で説明しているので、詳細は省略する。

【０２８９】

このように、ホームサーバ５１はコンテンツ利用権を購入し、課金情報はホームサーバ５１側で保存し、利用権は据置機器５２に引き渡される。

【０２９０】

図７５は、ホームサーバ５１が、既に購入済みのコンテンツ利用権を、別の利用形態に変更して購入するための処理を示したフローチャートである。図７５のステップＳ２４０からステップＳ２４５までは、図６７で説明した処理と同様であるため、その説明は省略する。ステップＳ２４６において、ホームサーバ５１の暗号処理部６５は、暗号処理部６５の外部メモリ制御部９７に、利用権変更するコンテンツの使用許諾条件情報を読み出させる。外部メモリ６７からのデータの読み出しは、図６８を参照して説明したので、その詳細は省略する。ステップＳ２４６で正常に使用許諾条件情報が読み出せた場合には、ステップＳ２４７へ進む。

【０２９１】

ステップＳ２４７において、ホームサーバ５１の上位コントローラ６２は、表示手段６４を用いて利用権内容変更可能なコンテンツの情報（例えば、利用権内容変更可能な利用形態や価格など）を表示し、ユーザは入力手段６３を用いて利用権内容更新条件を選択する。入力手段６３から入力された信号はホームサーバ５１の上位コントローラ６２に送信され、上位コントローラ６２は、その信号に

基づいて利用権内容変更コマンドを生成し、利用権内容変更コマンドをホームサーバ５１の暗号処理部６５に入力する。これを受信した暗号処理部６５は、ステップＳ２４３で受信した取扱方針、ステップＳ２４５で受信した価格情報およびステップＳ２４７で読み出した使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

【０２９２】

ステップＳ２４８は、図６７のステップＳ１７１と同様なため、その詳細な説明は省略する。ステップＳ２４９において、暗号処理部６５の制御部９１は、ステップＳ２４７で生成した使用許諾条件情報を、暗号処理部６５の外部メモリ制御部９７に出力する。外部メモリ制御部９７は、受信した使用許諾条件情報を外部メモリ６７に上書き更新する。外部メモリ制御部９７の外部メモリ６７への書き換え（更新）方法は、図７０で説明したので、その詳細は省略する。

【０２９３】

ステップＳ２４６において、外部メモリ６７に、権利内容変更コマンドに付加されたコンテンツＩＤに対応する使用許諾条件情報が見つからなかった場合、または、使用許諾条件情報が記憶されている外部メモリの記憶ブロックに改竄が発見された場合（図６８を参照して説明済み）、ステップＳ２５１へ進み、所定のエラー処理を行う。

【０２９４】

このように、ホームサーバ５１は、既に購入した権利（使用許諾権条件情報に記述されている）と、取扱方針および価格情報を用いて新たな権利を購入し、利用権内容を変更することができる。

【０２９５】

図７６及び図７７は、取扱方針および価格情報のルール部分の具体例を示したものである。図７６において、取扱方針は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益率から構成され、この取扱方針には例えば５つのルールが記述されている。ルール１は、権利項目が利用権内容番号１であるから、図４４より、その権利は再生権、時間・回数制限なしの権利であることがわ

かる。また、パラメータの項目には、特に記述がないことがわかる。最低販売価格は￥３５０であり、コンテンツプロバイダ２の取り分は、価格の３０％である。ルール２は、権利項目が利用権内容番号２であるから、図４４より、その権利は再生権、時間制限有り、回数制限なしの権利であることがわかる。また、利用可能期間が１時間であることが、パラメータの項目からわかる。最低販売価格は￥１００であり、コンテンツプロバイダ２の取り分は、価格の３０％である。ルール３は、権利項目が利用権内容番号６であるから、図４４より、その権利は複製権（コピー制御信号なし）、時間制限なし、回数制限ありの権利であることがわかる。また、利用可能回数が１回であることが、パラメータの項目からわかる。最低販売価格は￥３０であり、コンテンツプロバイダ２の取り分は、価格の３０％である。

【０２９６】

ルール４は、権利項目が利用権内容番号１３であるから、図４４より、その権利は利用内容変更であることがわかる。変更可能なルール番号は、＃２（再生権、時間制限有り、回数制限なし）から＃１（再生権、時間・回数制限なし）であることがパラメータの項目からわかる。最低販売価格は￥２００であり、コンテンツプロバイダ２の取り分は、価格の２０％である。最低販売価格がルール１より低く提示してあるのは、既に購入している権利を下取りして再購入すると考えているからであり、コンテンツプロバイダ２の取り分がルール１より低く提示してあるのは、実際の作業をする電子配信サービスセンタ１の取り分を増やすためである（コンテンツプロバイダ２は、権利内容変更時には作業がないため）。

【０２９７】

ルール５は、権利項目が利用権内容番号１４であるから、図４４より、その権利は再配布であることがわかる。再配布可能条件は、ルール番号＃１（再生権、時間・回数制限なし）を持っている機器が、ルール番号＃１（再生権、時間・回数制限なし）を購入して再配布することであることが、パラメータの項目からわかる。最低販売価格は￥２５０であり、コンテンツプロバイダ２の取り分は、価格の２０％である。最低販売価格がルール１より低く提示してあるのは、既に購入している権利をもつ機器が、同一コンテンツにつき再購入すると考えているか

らであり、コンテンツプロバイダ２の取り分がルール１より低く提示してあるのは、実際の作業をする電子配信サービスセンタ１の取り分を増やすためである（コンテンツプロバイダ２は、再配付時には作業がないため）。

【０２９８】

図７７において、価格情報は利用権ごとに整理番号として付けられたルール番号、パラメータ及び価格情報から構成され、この価格情報にも例えば５つのルールが記述されている。ルール１は、取扱方針のルール＃１に対する価格情報で、利用権内容番号＃１を購入する際に、価格が￥５００で、サービスプロバイダ３の取り分が３０％であることを示す。従って、ユーザが支払う￥５００は、コンテンツプロバイダ２が￥１５０、サービスプロバイダ３が￥１５０、電子配信サービスセンタ１が￥２００取ることになる。ルール２からルール５までも同様であるので、その詳細は省略する。

【０２９９】

なお、ルール４、５において、サービスプロバイダ２の取り分がルール１に比べて少ないのは、サービスプロバイダ２の配信作業をユーザ機器が代行して行っており、代金の回収は電子配信サービスセンタ１が行っているためである。

【０３００】

また本例ではルール番号が＃１から＃５へと連番となっているが、必ずしもその必要はない。作成者はルール番号ごとに利用権内容番号とパラメータを設定しておき、そこから抽出したものを並べるため、一般には連番にならない。

【０３０１】

図７８は、図７５で説明した権利内容変更を行う際の具体的な例を示したものである。取扱方針は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益率から構成され、価格情報は利用権ごとに整理番号として付けられたルール番号、パラメータ及び価格情報から構成され、使用許諾条件情報は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータから構成されている。ホームサーバ５１は、既にルール番号＃２の再生権、時間制限ありの権利を購入しており、権利内容を示す使用許諾条件

情報には、ルール番号＃２が記述されており、利用可能時間は残り３０分で、今まで積算して２時間分の購入を行っていることを示している。今、時間制限ありから時間制限なしに変更しようとした場合、取扱方針のルール３、価格情報のルール３および使用許諾条件情報から￥２００で再生権、時間・回数制限なしに変更でき、使用許諾条件情報は、ルール番号＃１、利用権内容番号の再生権、時間・回数制限なしに変わることがわかる（利用権内容番号＃１の場合のパラメータに関しては、後述する。また、本例で言えば、直接再生権、時間・回数制限なしを買う場合に比べ、一度、時間制限ありの権利を買ってから権利内容変更したほうが安くなってしまっている。このため、積算利用時間を見て割り引くようにした方がよい）。

【０３０２】

図７９は、ホームサーバ５１が据置機器５２のために、コンテンツ利用権を購入し、その利用権を再配布する処理の詳細を説明したフローチャートである。ステップＳ２６０からステップ２６４は、図７４のステップＳ２２０からステップＳ２２５と同様なため、その詳細な説明は省略する。ステップＳ２６５において、ホームサーバ５１の暗号処理部６５は、暗号処理部６５の外部メモリ制御部９７に、再配布しようとするコンテンツに対応する使用許諾条件情報および保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}を、外部メモリ６７から読み出させる。外部メモリ制御部９７による外部メモリ６７の読み出し方法については、図６８で説明したので、その詳細は省略する。読み出しに成功した場合は、ステップＳ２６６に進む。

【０３０３】

ステップＳ２６６において、ホームサーバ５１の上位コントローラ６２は、表示手段６４を用いて再配布可能なコンテンツの情報（例えば、再配布可能なコンテンツの利用形態や価格など）を表示し、ユーザは入力手段６３を用いて再配付条件を選択する。なお、この選択処理は、予め再配付処理スタート時に行うようにしても良い。入力手段６３から入力された信号はホームサーバ５１の上位コントローラ６２に送信され、上位コントローラ６２は、その信号に基づいて再配布コマンドを生成し、再配布コマンドをホームサーバ５１の暗号処理部６５に入力

する。これを受信した暗号処理部６５は、ステップＳ２６４で受信した取扱方針、価格情報およびステップＳ２６５で読み出した使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

【０３０４】

ステップＳ２６７は、図６７のステップＳ１７１と同様なため、その詳細な説明は省略する。ステップＳ２６８において、暗号処理部６５の制御部９１は、ステップＳ２６５で読み出した保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}を、暗号／復号化モジュール９６の復号化ユニット１１１で、記憶モジュール９２から供給された保存鍵K_{save}を用いて復号化する。そして、暗号処理部６５の制御部９１は、暗号／復号化モジュール９６の暗号化ユニット１１２で、ステップＳ２６０の相互認証時に据置機器５２と共有した一時鍵K_{temp}を用いてコンテンツ鍵K_{co}を再暗号化する。最後に、暗号／復号化モジュール９６の署名生成ユニット１１４は、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}と、ステップＳ２６６で生成した新しい使用許諾条件情報に対応した署名を生成し、暗号処理部６５の制御部９１に返送する。

【０３０５】

ステップＳ２６９からステップＳ２７２の処理は、図７４のステップＳ２２９からステップＳ２３２と同様なため、その詳細は省略する。

【０３０６】

このように、ホームサーバ５１は、自己の保持する利用権（使用許諾条件情報）と取扱方針、価格情報から新しい使用許諾条件情報を作り出し、自己の保持するコンテンツ鍵K_{co}、コンテンツとともに据置機器５２へ送信することで、コンテンツの再配布が行える。

【０３０７】

図８０は、ホームサーバ５１が据置機器５２のために、使用許諾条件情報、コンテンツ鍵K_{co}を送信し、据置機器５２でコンテンツ利用権を購入する処理の詳細を説明したフローチャートである。ステップＳ２８０において、据置機器５２の暗号処理部７３は、暗号処理部７３の記憶モジュールに記憶されている課金情報の課金の合計が、上限に達しているか否か判定し、上限に達していなかった場

合にはステップＳ２８１に進む（なお、課金合計上限で判定するのではなく、課金処理件数の上限で判定するようにしても良い）。

【０３０８】

ステップＳ２８１において、据置機器５２の上位コントローラ７２は、据置機器５２の小容量記憶部７５から読み出した登録情報を据置機器５２の暗号処理部７３に入力する。登録情報を受信した暗号処理部７３は、図示せぬ暗号／復号化モジュールの署名検証ユニットで登録情報の署名を検証した後、据置機器５２のＩＤに対する「購入処理」の項目が「購入可」になっているか判定し、「購入可」であった場合にはステップＳ２８２に進む。

【０３０９】

ステップＳ２８２は、図７４のステップＳ２２０と同様なため、その詳細は省略する。ステップＳ２８３は、図７４のステップＳ２２１と同様なため、その詳細は省略する（ホームサーバ５１は据置機器５２が登録されているか否かを判定し、据置機器５２はホームサーバ５１が登録されているか否かを判定する）。ステップＳ２８４は、図７９のステップＳ２６５と同様なため、その詳細は省略する。ステップＳ２８５は、図７９のステップＳ２６８と同様なため、その詳細は省略する。ステップＳ２８６において、暗号処理部６５の制御部９１は、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}と、ステップＳ２８４で読み出した使用許諾条件情報に対し、暗号／復号化モジュール９６の署名生成ユニット１１４を用いて署名を生成し、上位コントローラ６２に送信する。一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}、使用許諾条件情報およびそれらの署名を受信したホームサーバ５１の上位コントローラ６２は、大容量記憶部６８からコンテンツ鍵K_{co}で暗号化されたコンテンツ、必要に応じて取扱方針とその署名、価格情報とその署名を読み出し、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}、使用許諾条件情報、それらの署名、コンテンツ鍵K_{co}で暗号化されたコンテンツ、取扱方針とその署名および価格情報とその署名を据置機器５２に送信する。

【０３１０】

ステップＳ２８７は、図７４のステップＳ２３０と同様なため、その詳細は省略する。ステップＳ２８８は、図７４のステップＳ２２５と同様なため、その詳

細は省略する。ステップＳ２８９において、据置機器５２の上位コントローラ７２は、表示手段７８を用いて再配布可能なコンテンツの情報（例えば、再配布可能なコンテンツの利用形態や価格など）を表示し、ユーザは入力手段７７を用いて再配付条件を選択する。なお、この選択処理は予め再配付処理スタート時に行うようにしても良い。入力手段７７から入力された信号は据置機器５２の上位コントローラ７２に送信され、上位コントローラ７２は、その信号に基づいて再配布コマンドを生成し、再配布コマンドを据置機器５２の暗号処理部７３に入力する。これを受信した暗号処理部７３は、ステップＳ２８６で受信した取扱方針、価格情報および使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

【０３１１】

ステップＳ２９０において、据置機器５２の暗号処理部７３は、ステップＳ２８９で生成した課金情報を図示せぬ暗号処理部７３の記憶モジュールに保存する。ステップＳ２９１において、据置機器５２の暗号処理部７３は、ステップＳ２８６で受信した一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}を、図示せぬ暗号処理部７３の復号化ユニットで、ステップＳ２８２で共有した一時鍵K_{temp}を用いて復号化する。そして、据置機器５２の暗号処理部７３は、図示せぬ暗号処理部７３の暗号化ユニットで、図示せぬ暗号処理部７３の記憶モジュールから供給された保存鍵$K_{save}2$を用いてコンテンツ鍵K_{co}を暗号化する。

【０３１２】

ステップＳ２９２において、据置機器５２の暗号処理部７３は、ステップＳ２８９で生成した使用許諾条件情報およびステップＳ２９１で生成した保存鍵$K_{save}2$で暗号化されたコンテンツ鍵K_{co}を図示せぬ、暗号処理部７３の外部メモリ制御部に送信する。使用許諾条件情報および保存鍵$K_{save}2$で暗号化されたコンテンツ鍵K_{co}を受信した外部メモリ制御部は、使用許諾条件情報および保存鍵$K_{save}2$で暗号化されたコンテンツ鍵K_{co}を外部メモリ７９に書き込む。書き込む際の改竄チェックについては、図６９を用いて説明したので、その詳細は省略する。

【０３１３】

このように、据置機器５２は、ホームサーバ５１の保持する利用権（使用許諾条件情報）、取扱方針、価格情報、コンテンツ鍵K_{co}、コンテンツをホームサーバ５１から受信し、据置機器５２で新しい使用許諾条件情報を作り出すことにより、コンテンツの再配布を受けることができる。

【０３１４】

図８１は、管理移動権について説明した図である。管理移動とは、機器１から機器２へ再生権を移動できる動作のことで、機器１から機器２へ権利が移動することは通常の移動と同じであるが、機器２は受け取った再生権を再移動することができない点で通常の移動と異なる（通常の移動と同様に、再生権を移動した後の機器１は、再生権の再移動できない）。再生権を管理移動で受け取った機器２は、再生権を機器１に返還することができ、返還された後は、機器１は再度再生権の移動ができ、機器２は引き続きできない。これらを実現するため、使用許諾条件情報に管理移動権の購入者および現在の管理移動権の保持者を管理させている（ここでは、利用権内容番号＃１を持っている場合にのみ管理移動できることを想定しているが、利用権内容番号＃２においても拡張できる）。

【０３１５】

図８１において、取扱方針のルール１は、図７８で説明しているので、その詳細は省略する。ルール２は、権利項目が利用権内容番号１６であるから、図４４より、その権利は管理移動権であることがわかる。また、パラメータの項目には、特に記述がないことがわかる。最低販売価格は￥１００であり、コンテンツプロバイダ２の取り分は、価格の５０％である。コンテンツプロバイダ２の取り分がルール１より高く提示してあるのは、サービスプロバイダ３は実際の作業を全く行わないため、その分をコンテンツプロバイダ２への取り分に回したためである。

【０３１６】

図８１において、価格情報のルール１は、図７８で説明しているので、その詳細は省略する。ルール２は、取扱方針のルール＃２に対する価格情報で、利用権内容番号＃１６を購入する際に、価格が￥１００で、サービスプロバイダ３の取

り分が０％であることを示す。従って、ユーザが支払う￥１００は、コンテンツプロバイダ２が￥５０、サービスプロバイダ３が￥０、電子配信サービスセンタ１が￥５０取ることになる。

【０３１７】

図８１において、ユーザはまずルール番号＃１（再生権、時間・回数制限無し）を購入する。ただし、このとき管理移動権は持っていない（図８１の（ａ）の状態）。次に、ユーザは管理移動権を購入する（これらの動作は一瞬なため、ユーザは一括して購入したように見える）。使用許諾条件のルール番号は、購入者を示す暗号処理部のＩＤ（以下購入者とする）がＩＤ１（例えば、ホームサーバ５１のＩＤ）、再生権を保有する暗号処理部のＩＤ（以下保持者とする）がＩＤ２になる（図８１の（ｂ）の状態）。これを、管理移動を行って据置機器５２に移した場合、ホームサーバ５１の持つ使用許諾条件情報のルール部は、購入者はＩＤ１のままだが、保持者がＩＤ２に変化する。また、管理移動により再生権を受信した据置機器５２の持つ使用許諾条件情報のルール部は、購入者はＩＤ１、保持者はＩＤ２となり、ホームサーバ５１の使用許諾条件情報と一緒になっている。

【０３１８】

図８２は、管理移動権の移動処理の詳細を説明するフローチャートである。図８２において、ステップＳ３００は、図７４のステップＳ２２０と同様なため、その詳細は省略する。また、ステップＳ３０１は図７４のステップＳ２２１と同様なため、その詳細は省略する。ステップＳ３０２は図７５のステップＳ２４６と同様であため、その詳細は省略する。ステップＳ３０３において、ホームサーバ５１の暗号処理部６５は、読み出した使用許諾条件情報内のルール部を検査し、使用権が再生権、時間・回数制限なし、管理移動権ありになっているか判定する。管理移動権があると判定された場合、ステップＳ３０４に進む。

【０３１９】

ステップＳ３０４において、暗号処理部６５の制御部９１は、管理移動権の購入者および保持者が、共にホームサーバ５１のＩＤになっているか判定する。管理移動権の購入者および保持者が、共にホームサーバ５１のＩＤになっていると

判定された場合には、ステップＳ３０５に進む。ステップＳ３０５において、暗号処理部６５の制御部９１は、使用許諾条件情報の管理移動権の保持者を据置機器５２のＩＤに書き換える。ステップＳ３０６において、暗号処理部６５の制御部９１は、ステップＳ３０５で書き換えた使用許諾条件情報を暗号処理部６５の外部メモリ制御部９７に出力する。使用許諾条件情報を受信した暗号処理部６５の外部メモリ制御部９７は、外部メモリ６７に使用許諾条件情報を上書き保存する。外部メモリ６７のデータを書き換え保存する方法については、図７０で説明したので、その詳細は省略する。ステップＳ３０７からステップＳ３１１までは、図７９のステップＳ２６８からステップＳ２７２と同様なため、その詳細は省略する。

【０３２０】

ステップＳ３０３で使用許諾条件情報に管理移動権が含まれていなかった場合、ステップＳ３０４で管理移動権の購入者または保持者がホームサーバ５１でなかった場合は、処理を中断する。

【０３２１】

このように、ホームサーバ５１から据置機器５２にコンテンツを再生するための権利を移動することができる。

【０３２２】

図８３は、現在管理移動権を所持している据置機器５２から、管理移動権の購入者であるホームサーバ５１に、管理移動権を返還させる処理について説明したフローチャートである。図８３において、ステップＳ３２０は、図７４のステップＳ２２０と同様なため、その詳細は省略する。ステップＳ３２１は図７４のステップＳ２２１と同様であため、その詳細は省略するが、ホームサーバ５１と据置機器５２双方で相手のＩＤが登録されているか検査しているものとする。登録されていると判定された場合、ステップＳ３２２に進む。ステップＳ３２２は、図７５のステップＳ２４６と同様であるため、その詳細は省略するが、ホームサーバ５１と据置機器５２双方で同一のコンテンツＩＤのデータを読み出していることとする。外部メモリからデータが正しく読めた場合には、ステップＳ３２３に進む。ステップＳ３２３は、図８２のステップＳ３０３と同様であるため、そ

の詳細は省略するが、ホームサーバ５１と据置機器５２双方で管理移動権があるか判定していることとする。管理移動権があると判定された場合には、ステップＳ３２４に進む。

【０３２３】

ステップＳ３２４において、ホームサーバ５１の暗号処理部６５は、管理移動権の購入者がホームサーバ５１のＩＤになっていて、保持者が据置機器５２のＩＤになっているか判定する。管理移動権の購入者がホームサーバ５１のＩＤになっていて、保持者が据置機器５２のＩＤになっていると判定された場合には、ステップＳ３２５に進む。同様に、据置機器５２の暗号処理部７３は、管理移動権の購入者がホームサーバ５１のＩＤになっていて、保持者が据置機器５２のＩＤになっているか判定する。管理移動権の購入者がホームサーバ５１のＩＤになっていて、保持者が据置機器５２のＩＤになっていると判定された場合には、ステップＳ３２５に進む。

【０３２４】

ステップＳ３２５において、据置機器５２の記録再生部７６は、記録メディア８０からコンテンツを削除する（ただし、暗号化されたデータが残るだけなので、無理に削除する必要はない）。ステップＳ３２６において、据置機器５２の暗号処理部７３は、図示せぬ暗号処理部７３の外部メモリ制御部に、外部メモリ７９に保存されている保存鍵$K_{save}2$で暗号化されたコンテンツ鍵K_{co}と使用許諾条件情報を削除させる。外部メモリ７９の照りの削除方法は図７１で説明したので、その詳細は省略する。

【０３２５】

ステップＳ３２７において、暗号処理部６５の制御部９１は、使用許諾条件情報の管理移動権の保持者をホームサーバ５１のＩＤに書き換えた使用許諾条件情報を生成する。ステップＳ３２８において、暗号処理部６５の制御部９１は、ステップＳ３２７で生成した使用許諾条件情報を、暗号処理部６５の外部メモリ制御部９７に出力する。使用許諾条件情報を受信した暗号処理部６５の外部メモリ制御部９７は、外部メモリ６７に使用許諾条件情報を上書き保存する。外部メモリ６７に書き換え保存する方法については、図７０で説明したので、その詳細は

省略する。

【０３２６】

ステップＳ３２１でホームサーバ５１または据置機器５２において、登録情報が改竄されていたり、相手の機器のＩＤが登録されていなかった場合、ステップＳ３２２でホームサーバ５１または据置機器５２において、外部メモリ内に所定のコンテンツに対するコンテンツ鍵または使用許諾条件情報が見つからなかったり、それらを含むメモリブロックが改竄されていた場合は、ステップＳ３２９へ進みエラー処理を行う。

【０３２７】

ステップＳ３２３でホームサーバ５１または据置機器５２において、使用許諾条件情報内に管理移動権がなかった場合、ステップＳ３２４でホームサーバ５１または据置機器５２において、購入者がホームサーバ５１で、保持者が据置機器５２でなかった場合は、処理を中断する。

【０３２８】

このように、据置機器５２からホームサーバ５１にコンテンツを再生するための権利をもどすことができる。

【０３２９】

なお、コンテンツおよびコンテンツ鍵K_{co}等を１つしか記述していないが、必要に応じて複数存在することとする。

【０３３０】

また、本例ではコンテンツプロバイダ２とサービスプロバイダ３が別々に扱われていたが、一つにまとめてしまってもよい。更にまた、コンテンツプロバイダ２の方式を、そのままサービスプロバイダ３に転用しても良い。

【０３３１】

（２）個別鍵の使用による暗号化処理

コンテンツプロバイダ２は、図９について上述したようにコンテンツを自ら作成したコンテンツ鍵で暗号化する。また、コンテンツプロバイダ２は、電子配信サービスセンタ１からコンテンツプロバイダ固有の個別鍵と、配送鍵で暗号化された個別鍵を受け取り、個別鍵によってコンテンツ鍵を暗号化する。かくしてコ

ンテンツプロバイダ２は、コンテンツ鍵で暗号化されたコンテンツと、個別鍵で暗号化されたコンテンツ鍵と、配送鍵で暗号化された個別鍵とをサービスプロバイダ３を介してユーザホームネットワーク５に供給する。

【０３３２】

ユーザホームネットワーク５では、電子配信サービスセンタ１から受け取った配送鍵を用いてコンテンツプロバイダ固有の個別鍵を復号化する。これにより、ユーザホームネットワーク５はコンテンツプロバイダ２からコンテンツプロバイダ固有の個別鍵で暗号化されて供給されるコンテンツ鍵を復号することができる。コンテンツ鍵を得たユーザホームネットワーク５は当該コンテンツ鍵によりコンテンツを復号することができる。

【０３３３】

ここで、個別鍵はコンテンツサーバごとに固有であるのに対して、配送鍵は一種類のみである。従って、ユーザホームネットワーク５は一種類の配送鍵だけを持っていれば、各コンテンツプロバイダからの個別鍵を復号することができる。従って、ユーザホームネットワーク５は各コンテンツプロバイダ固有の個別鍵を持つ必要がなくなり、配送鍵を持つだけですべてのコンテンツプロバイダのコンテンツを購入することができる。

【０３３４】

また、各コンテンツプロバイダは、配送鍵を持たないことにより、他のコンテンツプロバイダ固有の個別鍵（配送鍵で暗号化されている）を復号することができない。これによりコンテンツプロバイダ間でのコンテンツの盗用を防止し得る。

【０３３５】

ここで、以上の実施の形態の構成と、特許請求の範囲に記載の発明の各手段とを明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【０３３６】

すなわち、本発明の情報送信システムにおいては、コンテンツ等の情報を送信

するコンテンツ供給者又はコンテンツ販売業者（例えば、図８４のコンテンツ送信装置２００）が持つ個別鍵保存用メモリ（例えば、図８４の耐タンパメモリ２０１）、コンテンツ鍵K_{co}を個別鍵K_iで暗号化するための手段（例えば、図８４のデータ暗号部２０３）、コンテンツ鍵K_{co}の使用条件等を記述した取扱方針を生成するための手段（例えば、図８４の取扱方針生成部２０６）、各種データに対してディジタル署名を生成するための手段（例えば、図８４の署名生成部２０７）と、コンテンツを購入するユーザ（例えば、図８４のコンテンツ受信装置２１０）が持つ各種データに対して生成された署名データを検証する手段（例えば、図８４の署名検証部２２２）、コンテンツ鍵K_{co}の生成者を示すＩＤと取扱方針の生成者のＩＤとを比較するための手段（例えば、図８４の比較器２２６）、配送鍵を保存するための手段（例えば、図８４の耐タンパメモリ２２１）とを備える。

【０３３７】

また、本発明の情報送信システムにおいては、コンテンツ等の情報を送信するコンテンツ供給者又はコンテンツ販売業者（例えば、図８５のコンテンツ送信装置２００）が持つ個別鍵保存用メモリ（例えば、図８５の耐タンパメモリ２０１）、鍵証明書を保存するためのメモリ（例えば、図８５のメモリ２０２）、コンテンツ鍵K_{co}を個別鍵K_iで暗号化するための手段（例えば、図８５のデータ暗号部２０３）、コンテンツを購入するユーザ（例えば、図８５のコンテンツ受信装置２１０）が持つ各種データに対して生成された署名データを検証する手段（例えば、図８５の署名検証部２２２）、配送鍵を保存するための手段（例えば、図８５の耐タンパメモリ２２１）とを備える。

【０３３８】

（３）遠隔再生処理

コンテンツの再生権利を保持していない機器（例えば据置機器５２）でコンテンツを保持している機器（例えばホームサーバ５１）から再生コマンドを受け取り、コンテンツを再生する遠隔再生処理について説明する。

【０３３９】

図８６は遠隔再生処理手順を示し、まず、ユーザの入力操作によって遠隔再生

しようとするコンテンツのコンテンツＩＤが上位コントローラ６２に入力された後、ステップＳ４０１において、ホームサーバ５１と据置機器５２は相互認証する。相互認証処理は、図５２で説明した処理と同様であるため、説明を省略する。ステップＳ４０２において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した登録情報を、ホームサーバ５１の暗号処理部６５に検査させる。上位コントローラ６２から登録情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５に、登録情報に付加されている署名を、暗号処理部６５の記憶モジュール９２から供給された認証局２２の公開鍵で検証させる。署名の検証に成功した後、「登録」の項目が「登録可」になっているか判定し、「登録可」になっていると判定された場合にはステップＳ４０３に進む。なお、据置機器５２側でも登録情報を検査し、ホームサーバ５１が「登録可」になっていることを判定している。

【０３４０】

ステップＳ４０３において上位コントローラ６２は遠隔再生しようとするコンテンツのコンテンツＩＤを含む再生コマンドを生成し、続くステップＳ４０４において、ホームサーバ５１の暗号処理部６５は、暗号処理部６５の外部メモリ制御部９７に、遠隔再生しようとするコンテンツに対応する使用許諾条件情報及び保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}を、外部メモリ６７から読み出させる。外部メモリ制御部９７による外部メモリ６７からのデータ読み出し方法については、図６８で説明した通りであり、その詳細は省略する。読み出しに成功した場合、ステップＳ４０５に進む。

【０３４１】

ステップＳ４０５において、暗号／復号化モジュール９６の復号化ユニット１１１は、外部メモリ６７から読み出したコンテンツ鍵K_{co}を、記憶モジュール９２から供給された保存鍵K_{save}で復号化する。ステップＳ４０６において、暗号／復号化モジュール９６の暗号化ユニット１１２は、一時鍵K_{temp}でコンテンツ鍵K_{co}を暗号化した後、ステップＳ４０７において再生コマンドを一時鍵K_{temp}で暗号化する。

【０３４２】

ホームサーバ５１は続くステップＳ４０８において、遠隔再生しようとするコンテンツ（コンテンツ鍵K_{co}で暗号化されている）を大容量記憶部６８から読み出して、これを上述のステップＳ４０６及びＳ４０７において一時鍵K_{temp}で暗号化されたコンテンツ鍵及び再生コマンドと共に据置機器５２に送信する。

【０３４３】

ステップＳ４０９において、据置機器５２はホームサーバ５１から受け取ったコンテンツ鍵及び再生コマンドを一時鍵K_{temp}で復号化し、ステップＳ４１０において暗号処理部７３と伸張部７４は相互認証を行い、一時鍵$K_{temp}2$を共有する。そしてステップＳ４１１において暗号処理部７３は上述のステップＳ４１０において伸張部７４と共有した一時鍵$K_{temp}2$でコンテンツ鍵K_{co}及び再生コマンドを暗号化する。ステップＳ４１２において、暗号処理部７３は一時鍵$K_{temp}2$で暗号化されたコンテンツ鍵K_{co}及び再生コマンドを伸張部７４に送信し、伸張部７４はステップＳ４１３においてコンテンツ鍵K_{co}及び再生コマンドを一時鍵$K_{temp}2$で復号化する。

【０３４４】

伸張部７４はステップＳ４１４において、ホームサーバ５１から上述のステップＳ４０８においてホームサーバ５１から受け取ったコンテンツを上述のステップＳ４１３において復号化された再生コマンドに従って上述のステップＳ４１３において復号化されたコンテンツ鍵K_{co}で復号化する。そして伸張部７４は当該復号化されたコンテンツをステップＳ４１５において所定の方式、例えばＡＴＲＡＣなどの方式により伸張する。ステップＳ４１６において、上位コントローラ７２は暗号処理部７３から指示されたデータを電子透かしの形でコンテンツに挿入する。因みに、暗号処理部７３から伸張部７４へ渡されるデータは、コンテンツ鍵K_{co}及び再生コマンドだけではなく、再生条件（アナログ出力、ディジタル出力、コピー制御信号付き出力（ＳＣＭＳ））、コンテンツ利用権を購入した機器ＩＤなども含まれている。挿入するデータは、このコンテンツ利用権を購入した機器のＩＤ、つまりは、使用許諾条件情報内の機器ＩＤなどである。ステップＳ４１７において、伸張部７４は、図示せぬスピーカを介して音楽を再生する。

【０３４５】

以上の構成において、ホームサーバ５１はコンテンツと当該コンテンツの再生コマンド及びコンテンツ鍵K_{co}を据置機器５２に送信することにより、コンテンツの再生権利を保持していない据置機器５２は、再生コマンド及びコンテンツ鍵K_{co}を用いてコンテンツを再生することができる。従って、以上の構成によれば、コンテンツを保持する機器（コンテンツの再生権利を有する機器）に接続された複数の機器（据置機器等）において、コンテンツを再生することができる。

【０３４６】

（４）予約購入処理

配送鍵の有効期限が切れる前にコンテンツの鍵変換を予め行っておき、コンテンツの購入予約を行うホームサーバの予約購入処理について説明する。図８７に示す予約購入処理手順のステップＳ４５１において、ホームサーバ５１は登録情報更新判断処理を行い、ステップＳ４５２に進む。登録情報更新判断処理については、図６１及び図６２で説明した通りであり、その詳細説明は省略する。但し、予約購入処理においては、図６１のステップＳ６０１やＳ６０２で述べた購入個数や購入金額に基づく登録情報更新タイミングの判断は行わなくても良い。

【０３４７】

ステップＳ４５２において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した登録情報をホームサーバ５１の暗号処理部６５に入力する。登録情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で登録情報の署名を検証した後、ホームサーバ５１のＩＤに対する「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか否かを判定し、「購入可」及び「登録可」であった場合にはステップＳ４５３に進む。ステップＳ４５３において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出したコンテンツプロバイダ２の公開鍵証明書をホームサーバ５１の暗号処理部６５に入力する。コンテンツプロバイダ２の公開鍵証明書を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でコンテンツプロバイダ２の公開鍵証明書の署名を検証した後、公開鍵証明書からコンテンツプ

ロバイダ２の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、上位コントローラ６２はステップＳ４５４に進む。

【０３４８】

ステップＳ４５４においてホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出したコンテンツ鍵K_{co}をホームサーバ５１の暗号処理部６５に入力する。コンテンツ鍵K_{co}を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でコンテンツ鍵K_{co}の署名を検証し、改ざんがなされていないことが確認された場合には、ステップＳ４５５に進む。

【０３４９】

ステップＳ４５５において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した個別鍵K_iをホームサーバ５１の暗号処理部６５に入力する。個別鍵K_iを受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で個別鍵K_iの署名を検証し、改ざんがなされていないことが確認された場合には、ステップＳ４５６に進む。

【０３５０】

ここで、個別鍵K_iで暗号化されたコンテンツ鍵K_{co}及び配送鍵K_dで暗号化された個別鍵K_i全体に対して１つの署名がついている場合は、Ｓ４５４及びＳ４５５を１つに合わせることができ署名検証処理を簡略化できる。

【０３５１】

ステップＳ４５６において、暗号処理部６５の制御部９１は、ステップＳ４５５で入力された個別鍵K_iを、暗号／復号化モジュール９６の復号化ユニット１１１で、記憶モジュール９２から供給された配送鍵K_dを用いて復号化する。次に、暗号処理部６５の制御部９１は、ステップＳ４５４で入力されたコンテンツ鍵K_{co}を、暗号／復号化モジュール９６の復号化ユニット１１１で、先ほど復号化した個別鍵K_iを用いて復号化する。最後に、暗号処理部６５の制御部９１は、暗号／復号化モジュール９６の暗号化ユニット１１２で、記憶モジュール９２から供給された保存鍵K_{save}を用いてコンテンツ鍵K_{co}を暗号化する。

【０３５２】

ステップＳ４５７において、保存鍵K_{save}で暗号化されたコンテンツ鍵K_{co}は、暗号処理部６５の外部メモリ制御部９７を経由して外部メモリ６７に保存される。

【０３５３】

また、ステップＳ４５２でホームサーバ５１が購入処理できない機器であると判定された場合、又はステップＳ４５３でコンテンツプロバイダ２の公開鍵証明書の署名が正しくないと判定された場合、又はステップＳ４５４で個別鍵K_iで暗号化されたコンテンツ鍵K_{co}の署名が正しくないと判定された場合、又はステップＳ４５５で配送鍵K_dで暗号化された個別鍵K_iの署名が正しくないと判定された場合、ホームサーバ５１はステップＳ４５８に進み、エラー処理を行う。

【０３５４】

以上のように、ホームサーバ５１は、コンテンツ鍵K_{co}を個別鍵K_iで復号化した後、コンテンツ鍵K_{co}を保存鍵K_{save}で再暗号化し、外部メモリ６７に記憶させる。この予約購入処理は、実際にコンテンツを購入しないので、図６７について上述した購入処理のうち、ステップＳ１６１の登録情報更新判断処理のなかの課金情報についての処理、ステップＳ１６４に対応する購入コンテンツについての処理、ステップＳ１６７に対応する取扱い方針についての処理、ステップＳ１６８に対応するサービスプロバイダの公開鍵検証についての処理、ステップＳ１６９に対応する価格情報の署名検証についての処理、ステップＳ１７０乃至ステップＳ１７２に対応する課金情報及び使用許諾条件情報の保存処理は行わなくても良い。

【０３５５】

因みに、図８７の予約購入処理の場合、ホームサーバ５１は使用許諾条件情報の作成は行わなかったが、これに代えて使用許諾条件情報を作成しその利用権内容番号（すなわち権利項目）を初期値等の権利を持っていない状態（例えば、存在しない＃０など）としておくようにしても良い。

【０３５６】

このようにして、予約購入処理では、ホームサーバ５１は配送鍵K_dの有効期

限が切れる前にコンテンツ鍵K_{co}を外部メモリ６７に保存しておくことにより、当該保存されたコンテンツ鍵K_{co}によって暗号化されたコンテンツについて、配送鍵K_dの期限に関わらず購入することができる。

【０３５７】

ここで、ホームサーバ５１において外部メモリ６７にコンテンツ鍵K_{co}を　保存することにより購入の予約がなされたコンテンツの本購入処理について説明する。図８８に示す本購入処理手順のステップＳ４７１において、ホームサーバ５１は登録情報更新判断処理を行い、ステップＳ４７２に進む。登録情報更新判断処理については、図６１及び図６２で説明した通り、その詳細は、省略する。但し、本購入処理においては、図６１のステップＳ６０３で述べた配送鍵K_dに基づく登録情報更新タイミングの判断は行わなくて良い。

【０３５８】

ステップＳ４７２において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した登録情報をホームサーバ５１の暗号処理部６５に入力する。登録情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で登録情報の署名を検証した後、ホームサーバ５１のＩＤに対する「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか判定し、「購入可」及び「登録可」であった場合にはステップＳ４７３に進む。ステップＳ４７３において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出したコンテンツプロバイダ２の公開鍵証明書をホームサーバ５１の暗号処理部６５に入力する。コンテンツプロバイダ２の公開鍵証明書を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でコンテンツプロバイダ２の公開鍵証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ２の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、ステップＳ４７４に進む。

【０３５９】

ステップＳ４７４において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出したコンテンツをホームサーバ５

１の暗号処理部６５に入力する。コンテンツを受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でコンテンツの署名を検証し、改ざんがなされていないことが確認された場合には、ステップＳ４７５に進む。

【０３６０】

ステップＳ４７５において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した取扱方針をホームサーバ５１の暗号処理部６５に入力する。取扱方針を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で取扱方針の署名を検証し、改ざんがなされていないことが確認された場合には、ステップＳ４７６に進む。ステップＳ４７６において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出したサービスプロバイダ３の公開鍵証明書をホームサーバ５１の暗号処理部６５に入力する。サービスプロバイダ３の公開鍵証明書を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５でサービスプロバイダ３の公開鍵証明書の署名を検証した後、公開鍵証明書からサービスプロバイダ３の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、ステップＳ４７７に進む。

【０３６１】

ステップＳ４７７において、ホームサーバ５１の上位コントローラ６２は、ホームサーバ５１の大容量記憶部６８から読み出した価格情報をホームサーバ５１の暗号処理部６５に入力する。価格情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５で価格情報の署名を検証し、改ざんがなされていないことが確認された場合には、ステップＳ４７８に進む。

【０３６２】

ステップＳ４７８において、ホームサーバ５１の上位コントローラ６２は、表示手段６４を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段６３を用いて購入項目を選択する。なお、購入項目の選択処理は本購入処理に先立って行うようにしても良い。入力手

段６３から入力された信号はホームサーバ５１の上位コントローラ６２に送信され、上位コントローラ６２は、その信号に基づいて購入コマンドを生成し、購入コマンドをホームサーバ５１の暗号処理部６５に入力する。これを受信した暗号処理部６５は、ステップＳ４７５で入力された取扱方針及びステップＳ４７７で入力された価格情報から課金情報及び使用許諾条件情報を生成する。課金情報については、図４２で説明した通りであり、その詳細は省略する。また、使用許諾条件情報については、図４１で説明した通りであり、その詳細は省略する。

【０３６３】

ステップＳ４７９において、暗号処理部６５の制御部９１は、ステップＳ４７８で生成した課金情報を記憶モジュール９２に保存する。そしてステップＳ４８０において、暗号処理部６５の制御部９１は、ステップＳ４７８で生成した使用許諾条件情報を暗号処理部６５の外部メモリ制御部９７に送信する。使用許諾条件情報を受信した外部メモリ制御部９７は、外部メモリ６７の改ざんチェックを行った後、使用許諾条件情報を外部メモリ６７に書き込む。書き込む際の改ざんチェックについては、図６９について上述した通りであり、詳細説明は省略する（なお、権利なしの使用許諾条件情報がすでに書き込まれている場合には、図７０で説明した書き換え処理により使用許諾条件情報を書き換え更新する）。

【０３６４】

因みに、ステップＳ４７２でホームサーバ５１が購入処理できない機器であったり、登録されていないと判定された場合、又はステップＳ４７３でコンテンツプロバイダ２の公開鍵証明書の署名が正しくないと判定された場合、又はステップＳ４７４でコンテンツ鍵K_{co}で暗号化されたコンテンツの署名が正しくないと判定された場合、又はステップＳ４７５で取扱方針の署名が正しくないと判定された場合、又はステップＳ４７６でサービスプロバイダ３の公開鍵証明書の署名が正しくないと判定された場合、又はステップＳ４７７で価格情報の署名が正しくないと判定された場合、ホームサーバ５１はステップＳ４８１に進み、エラー処理を行う。

【０３６５】

以上のように、ホームサーバ５１ではユーザが購入選択したコンテンツについ

ての課金情報を記憶モジュール９２に記憶すると共に、使用許諾条件情報を外部メモリ６７に記憶することにより、コンテンツの本購入処理を終了する。この本購入処理では、図８７について上述した予約購入処理で既に行われたコンテンツ鍵K_{co}の署名検証（ステップＳ４５４）及び個別鍵K_iの署名検証（ステップＳ４５５）、並びにコンテンツ鍵K_{co}のかけ替え処理（ステップＳ４５６）は行わない。

【０３６６】

以上の構成において、ホームサーバ５１では配送鍵K_dが更新される前に予約購入処理によりコンテンツ鍵K_{co}を外部メモリ６７に保存しておくことにより、コンテンツ鍵K_{co}を復号化する際に必要となる配送鍵K_dが更新されても、コンテンツ鍵K_{co}は既に外部メモリ６７に保存されているので、配送鍵K_dの有効期限が切れてもコンテンツを購入することができる。

【０３６７】

（５）代理購入処理

登録情報(Registration List) が異なっている機器、すなわちグループが異なっている機器間においてコンテンツの授受を行う代理購入処理について説明する。この代理購入処理では、例えばホームサーバ５１と当該ホームサーバ５１に対してグループ外機器である携帯機器等との間でコンテンツを授受する場合について、ホームサーバ５１側で課金する場合と、グループ外機器で課金を行う場合をそれぞれ説明する。この場合、図１５について上述した据置機器５２をグループ外機器として説明する。

【０３６８】

図８９はホームサーバ５１がグループ外機器にコンテンツを渡し、ホームサーバ５１が課金処理を行う場合の処理手順を示し、ステップＳ５０１において、ホームサーバ５１とグループ外機器は、相互認証する。相互認証処理は、図５２で説明した処理と同様であるため、説明を省略する。ステップＳ５０２において、ホームサーバ５１とグループ外機器とは互いに登録情報を交換し、続くステップＳ５０３において互いに相手の登録情報を検査する。

【０３６９】

すなわち、ホームサーバ５１はグループ外機器から受け取った登録情報を、暗号処理部６５に検査させる。グループ外機器からの登録情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５に、登録情報に付加されている署名を、暗号処理部６５の記憶モジュール９２から供給された公開鍵で検証させる。署名の検証に成功した後、暗号処理部６５の制御部９１は、登録情報にグループ外機器のＩＤが登録され、「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか否かを判定する。また、ホームサーバ５１の登録情報を受け取ったグループ外機器も、同様にしてホームサーバ５１の登録情報にホームサーバ５１のＩＤが登録され、「登録」の項目が「登録可」になっているか否かを判定する。そして、互いに相手の機器が登録されていることが確認されると、ホームサーバ５１はステップＳ５０４に移る。

【０３７０】

ステップＳ５０４からステップＳ５１０は、図６７のステップＳ１６１からステップＳ１７１までと同様な処理なため、その詳細は省略する。

【０３７１】

ステップＳ５１１において、暗号処理部６５の制御部９１は、ステップＳ５０８で入力された配送鍵K_dで暗号化された個別鍵K_iを、暗号／復号化モジュール９６の復号化ユニット１１１で、記憶モジュール９２から供給された配送鍵K_dを用いて復号化する。次に、暗号処理部６５の制御部９１は、ステップＳ５０８で入力された個別鍵K_iで暗号化されたコンテンツ鍵K_{co}を、暗号／復号化モジュール９６の復号化ユニット１１１で、先ほど復号化した個別鍵K_iを用いて復号化する。そして、暗号処理部６５の制御部９１は、暗号／復号化モジュール９６の暗号化ユニット１１２で、ステップＳ５０１の相互認証時にグループ外機器と共有した一時鍵K_{temp}を用いてコンテンツ鍵K_{co}を再暗号化する。ステップＳ５１２において、暗号処理部６５の制御部９１は、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}と、ステップＳ５０９で生成した使用許諾条件情報に対し、暗号／復号化モジュール９６の署名生成ユニット１１４を用いて署名を生成し、上位コントローラ６２に送信する。一時鍵K_{temp}で暗号化されたコンテンツ鍵Ｋ

$_{co}$、使用許諾条件情報およびそれらの署名を受信したホームサーバ５１の上位コントローラ６２は、大容量記憶部６８からコンテンツ鍵K_{co}で暗号化されたコンテンツを読み出し、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}、使用許諾条件情報、それらの署名およびコンテンツ鍵K_{co}で暗号化されたコンテンツをグループ外機器に送信する。

【０３７２】

ステップＳ５１３において、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}、使用許諾条件情報、それらの署名およびコンテンツ鍵K_{co}で暗号化されたコンテンツを受信したグループ外機器は、コンテンツ鍵K_{co}で暗号化されたコンテンツをグループ外機器の記録再生部７６に出力する。コンテンツ鍵K_{co}で暗号化されたコンテンツを受信したグループ外機器の記録再生部７６は、コンテンツ鍵K_{co}で暗号化されたコンテンツを記録メディア８０に保存する。

【０３７３】

ステップＳ５１４において、グループ外機器の暗号処理部７３は、上述のステップＳ５１２でホームサーバから受け取った署名の検証を行うと共に、一時鍵K_{temp}で暗号化されたコンテンツ鍵K_{co}を、暗号／復号化モジュールの復号化ユニットで、ステップＳ５０１の相互認証時にホームサーバ５１と共有した一時鍵K_{temp}を用いて復号化する。そして、暗号処理部７３の制御部は、暗号／復号化モジュールの暗号化ユニットで、暗号処理部７３の記憶モジュールから供給された保存鍵$K_{save}2$を用いてコンテンツ鍵K_{co}を再暗号化する。

【０３７４】

ステップＳ５１５において、グループ外機器の暗号処理部７３は、保存鍵$K_{save}2$で暗号化されたコンテンツ鍵K_{co}とステップＳ５１３で受信した使用許諾条件情報を暗号処理部７３の外部メモリ制御部に送信し、外部メモリ７９に保存させる。外部メモリ制御部が外部メモリにデータを書き込む処理については、図６９で説明しているので、詳細は省略する。

【０３７５】

このように、ホームサーバ５１はコンテンツ利用権を購入し、課金情報はホームサーバ５１側で保存し、利用権はグループ外機器に引き渡される。これにより

、ホームサーバ５１はクループ外機器に引き渡したコンテンツ利用権についてその支払いを行うことになる。

【０３７６】

次に、図９０はホームサーバ５１がグループ外機器にコンテンツを渡し、グループ外機器が課金処理を行う場合の処理手順を示し、ステップＳ５５１においてグループ外機器は、暗号処理部７３（図１５）内に記憶されている課金情報の課金の合計が、上限に達しているか否か判定し、上限に達していなかった場合にはステップＳ５５２に進む（なお、課金合計上限で判定するのではなく、課金処理件数の上限で判定するようにしても良い）。

【０３７７】

ステップＳ５５２において、グループ外機器の上位コントローラ７２は、外部メモリ７９から読み出した登録情報を暗号処理部７３に入力する。登録情報を受信した暗号処理部７３は、その内部に設けられた暗号／復号化モジュールの署名検証ユニットで登録情報の署名を検証した後、グループ外機器（据置機器５２）のＩＤに対する「購入処理」の項目が「購入可」になっているか判定し、「購入可」であった場合にはステップＳ５５３に進む。

【０３７８】

ステップＳ５５３において、ホームサーバ５１とグループ外機器は、相互認証する。相互認証処理は、図５２で説明した処理と同様であるため、説明を省略する。ステップＳ５５４において、ホームサーバ５１とグループ外機器とは互いに登録情報を交換し、続くステップＳ５５５において互いに相手の登録情報を検査する。

【０３７９】

すなわち、ホームサーバ５１はグループ外機器から受け取った登録情報を、暗号処理部６５に検査させる。グループ外機器からの登録情報を受信した暗号処理部６５は、暗号／復号化モジュール９６の署名検証ユニット１１５に、登録情報に付加されている署名を、暗号処理部６５の記憶モジュール９２から供給された公開鍵で検証させる。署名の検証に成功した後、暗号処理部６５の制御部９１は、登録情報にグループ外機器のＩＤが登録され、「登録」の項目が「登録可」に

なっているか否かを判定する。また、ホームサーバ５１の登録情報を受け取ったグループ外機器も、同様にしてホームサーバ５１の登録情報にホームサーバ５１のＩＤが登録され、「登録」の項目が「登録可」になっているか否かを判定する。なお、同様の処理をグループ外機器も行っている。そして、互いに相手の機器が登録されていることが確認されると、ホームサーバ５１はステップＳ５５６に移る。

【０３８０】

ステップＳ５５６において、ホームサーバ５１の制御部９１は、外部メモリ制御部９７を介して外部メモリ６７から既に購入済のコンテンツ鍵を読み出し、続くステップＳ５５７においてコンテンツ鍵K_{co}を保存鍵K_{save}で復号化すると共に一時鍵K_{temp}で再暗号化し、それらの署名を生成する。

【０３８１】

ステップＳ５５８において、ホームサーバ５１は、Ｓ５５７で生成した保存鍵K_{temp}で暗号化されたコンテンツ鍵と大容量記憶部６８から読みだしたコンテンツ、取扱方針、価格情報をグループ外機器に送信する。ステップＳ５５９においてグループ外機器は、ホームサーバ５１から受け取ったコンテンツを記録メディア８０に保存する。

【０３８２】

ステップＳ５６０において、グループ外機器（据置機器５２）は取扱方針、価格情報等の署名を検証した後、ステップＳ５６１において、グループ外機器の上位コントローラ７２は、表示手段７８を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段７７を用いて購入項目を選択する。なお購入項目の選択処理は代理購入処理に先立って行うようにしても良い。入力手段７７から入力された信号は上位コントローラ７２に送信され、上位コントローラ７２は、その信号に基づいて購入コマンドを生成し、購入コマンドを暗号処理部７３に入力する。これを受信した暗号処理部７３は、ステップＳ５６０で入力された取扱方針および価格情報から課金情報および使用許諾条件情報を生成する。課金情報については、図４２で説明したので、その詳細は省略する。使用許諾条件情報については、図４１で説明したので、その詳

細は省略する。

【０３８３】

ステップＳ５６２において、暗号処理部７３は、ステップＳ５６１で生成した課金情報を暗号処理部７３内の記憶モジュールに保存する。ステップＳ５６３において、暗号処理部７３は、ステップＳ５５７で暗号化されたコンテンツ鍵について、署名を検証すると共に一時鍵K_{temp}で復号化し、保存鍵$K_{save}2$で再暗号化する。そしてステップＳ５６４において、保存鍵$K_{save}2$で暗号化されたコンテンツ鍵K_{co}は、暗号処理部７３から外部メモリ７９に保存される。

【０３８４】

このように、ホームサーバ５１は既に購入したコンテンツ利用権をグループ外機器に引き渡し、グループ外機器は課金情報も保存することにより、グループ外機器はグループ外のホームサーバ５１から引き渡されたコンテンツ利用権についてその支払いを行うことになる。

【０３８５】

以上の構成において、登録情報(Registration List) が異なっている機器間において、上述のステップＳ５０２及びステップＳ５５４について上述したように、互いの登録情報を交換することにより、登録された機器であることを確認した後一方の機器が有するコンテンツを他方の機器に引き渡すことができる。従って、以上の構成によれば、グループが異なる機器間においてコンテンツの授受を行うことができる。

【０３８６】

なお、上述の実施の形態においては、購入処理の際にコンテンツの署名を検証したが、処理に時間がかかるため省略する場合がある。また、取扱方針又は価格情報に、検証の必要性の有無を記述し、それに従つて動作する場合がある。

【０３８７】

【発明の効果】

上述のように本発明によれば、情報送信装置毎に個別の鍵を使用することができ、情報送信装置間のコンテンツデータの不正使用を防止することができ、情報受信装置は配送鍵を持つだけで各情報送信装置からのコンテンツデータを復号す

ることができる。

【図面の簡単な説明】

【図１】

本発明による電子音楽配信システムの全体構成を示すブロック図である。

【図２】

電子配信サービスセンタの構成を示すブロック図である。

【図３】

鍵の定期的な更新例を示す略線図である。

【図４】

鍵の定期的な更新例を示す略線図である。

【図５】

鍵の定期的な更新例を示す略線図である。

【図６】

鍵の定期的な更新例を示す略線図である。

【図７】

ユーザ登録データベースのデータ内容を示す略線図である。

【図８】

グループごとの登録情報を示す略線図である。

【図９】

コンテンツプロバイダの構成を示すブロック図である。

【図１０】

署名生成処理手順を示すフローチャートである。

【図１１】

署名検証処理手順を示すフローチャートである。

【図１２】

楕円曲線暗号化方法を示すフローチャートである。

【図１３】

楕円曲線暗号化の復号化処理を示すフローチャートである。

【図１４】

サービスプロバイダの構成を示すブロック図である。

【図１５】

ユーザホームネットワークの構成を示すブロック図である。

【図１６】

外部メモリ制御部の動作の説明に供する略線図である。

【図１７】

電子配信専用記録メディアの構成を示すブロック図である。

【図１８】

各機器の持つデータ内容を示すブロック図である。

【図１９】

記録メディアが保持するデータ内容を示すブロック図である。

【図２０】

システム全体のデータの流れを示す略線的ブロック図である。

【図２１】

公開鍵証明書の流れを示す略線的ブロック図である。

【図２２】

コンテンツプロバイダセキュアコンテナを示す略線図である。

【図２３】

コンテンツプロバイダセキュアコンテナを示す略線図である。

【図２４】

コンテンツプロバイダセキュアコンテナを示す略線図である。

【図２５】

コンテンツプロバイダセキュアコンテナを示す略線図である。

【図２６】

コンテンツプロバイダの公開鍵証明書を示す略線図である。

【図２７】

コンテンツプロバイダの公開鍵証明書を示す略線図である。

【図２８】

コンテンツプロバイダの公開鍵証明書を示す略線図である。

【図２９】

サービスプロバイダセキュアコンテナを示す略線図である。

【図３０】

サービスプロバイダセキュアコンテナを示す略線図である。

【図３１】

サービスプロバイダの公開鍵証明書を示す略線図である。

【図３２】

ユーザ機器の公開鍵証明書を示す略線図である。

【図３３】

シングルコンテンツの取扱方針を示す略線図である。

【図３４】

アルバムコンテンツの取扱方針を示す略線図である。

【図３５】

シングルコンテンツの取扱方針の他の例を示す略線図である。

【図３６】

アルバムコンテンツの取扱方針の他の例を示す略線図である。

【図３７】

シングルコンテンツの価格情報を示す略線図である。

【図３８】

アルバムコンテンツの価格情報を示す略線図である。

【図３９】

シングルコンテンツの価格情報の他の例を示す略線図である。

【図４０】

アルバムコンテンツの価格情報の他の例を示す略線図である。

【図４１】

使用許諾条件情報を示す略線図である。

【図４２】

課金情報を示す略線図である。

【図４３】

課金情報の他の例を示す略線図である。

【図４４】

利用権内容の一覧を示す略線図である。

【図４５】

利用権を示す略線図である。

【図４６】

シングルコンテンツを示す略線図である。

【図４７】

アルバムコンテンツを示す略線図である。

【図４８】

シングルコンテンツ用の鍵データを示す略線図である。

【図４９】

個別鍵の暗号化処理の説明に供するブロック図である。

【図５０】

アルバムコンテンツ用の鍵データを示す略線図である。

【図５１】

対称鍵技術を用いた相互認証処理を示すタイミングチャートである。

【図５２】

非対称鍵暗号技術を用いた相互認証処理を示すタイミングチャートである。

【図５３】

課金情報の送信動作を示す略線的ブロック図である。

【図５４】

利益分配処理動作を示す略線的ブロック図である。

【図５５】

コンテンツ利用実績の送信動作を示す略線的ブロック図である。

【図５６】

コンテンツの配布及び再生処理手順を示すフローチャートである。

【図５７】

コンテンツプロバイダへの送信処理手順を示すフローチャートである。

【図５８】

決済情報の登録処理手順を示すフローチャートである。

【図５９】

機器ＩＤの新規登録処理手順を示すフローチャートである。

【図６０】

機器の追加登録処理手順を示すフローチャートである。

【図６１】

登録情報の更新開始条件の判断処理を示すフローチャートである。

【図６２】

登録情報更新処理手順を示すフローチャートである。

【図６３】

据置機器による登録情報更新代理処理手順を示すフローチャートである。

【図６４】

据置機器による登録情報更新代理処理手順を示すフローチャートである。

【図６５】

セキュアコンテナの送信処理手順を示すフローチャートである。

【図６６】

セキュアコンテナの送信処理手順を示すフローチャートである。

【図６７】

ホームサーバの購入処理手順を示すフローチャートである。

【図６８】

データ読み出し時の改竄チェック処理手順を示すフローチャートである。

【図６９】

データ書込み時の改竄チェック処理手順を示すフローチャートである。

【図７０】

データ書換え時の改竄チェック処理手順を示すフローチャートである。

【図７１】

データ削除時の改竄チェック処理手順を示すフローチャートである。

【図７２】

ホームサーバによるコンテンツの再生処理手順を示すフローチャートである。

【図７３】

ホームサーバによるコンテンツの再生処理手順を示すフローチャートである。

【図７４】

ホームサーバによるコンテンツ利用権の代理購入処理手順を示すフローチャートである。

【図７５】

購入済利用者の内容変更処理手順を示すフローチャートである。

【図７６】

取扱方針のルール部の内容を示す略線図である。

【図７７】

価格情報のルール部の内容を示す略線図である。

【図７８】

権利内容の変更例を示す略線図である。

【図７９】

コンテンツ利用権の再配布処理手順を示すフローチャートである。

【図８０】

据置機器でのコンテンツ利用権購入処理手順を示すフローチャートである。

【図８１】

使用許諾条件情報のルール部の変遷を示す略線図である。

【図８２】

管理移動権の移動処理手順を示すフローチャートである。

【図８３】

管理移動権の返還処理手順を示すフローチャートである。

【図８４】

本発明による情報送信システムを示すブロック図である。

【図８５】

本発明による情報送信システムを示すブロック図である。

【図８６】

遠隔再生処理手順を示すフローチャートである。

【図８７】

予約購入処理手順を示すフローチャートである。

【図８８】

予約購入後の本購入処理手順を示すフローチャートである。

【図８９】

ホームサーバが課金する場合の代理購入処理手順を示すフローチャートである。

【図９０】

グループ外機器が課金する場合の代理購入処理手順を示すフローチャートである。

【図９１】

従来例を示すブロック図である。

【符号の説明】

１……電子配信サービスセンタ、２……コンテンツプロバイダ、３……サービスプロバイダ、４……ネットワーク、５……ユーザホームネットワーク、１０……電子音楽配信システム、１１……サービスプロバイダ管理部、１２……コンテンツプロバイダ管理部、１３……著作権管理部、１４……鍵サーバ、１５……経歴データ管理部、１６……利益分配部、１７……相互認証部、１８……ユーザ管理部、１９……課金請求部、２０……出納部、２１……監査部、２２……認証局、２３……コンテンツサーバ、２４……コンテンツオーサリング部、３１……コンテンツサーバ、３２……電子透かし付加部、３４……コンテンツ暗号部、３５……コンテンツ鍵生成部、３６……コンテンツ鍵暗号部、３７……取扱方針生成部、３８……署名生成部、３９……相互認証部、４１……コンテンツサーバ、４

２……証明書検証部、４３……署名検証部、４４……値付け部、４５……署名生成部、４６……相互認証部、５１……ホームサーバ、５２……据置機器、５３……携帯機器、６２、７２、８２……上位コントローラ、６５、７３、８３……暗号処理部、６６、７４、８４……伸張部、６７、７９、８５……外部メモリ、１２０……電子配信専用記録メディア。

【書類名】図面

【図１】

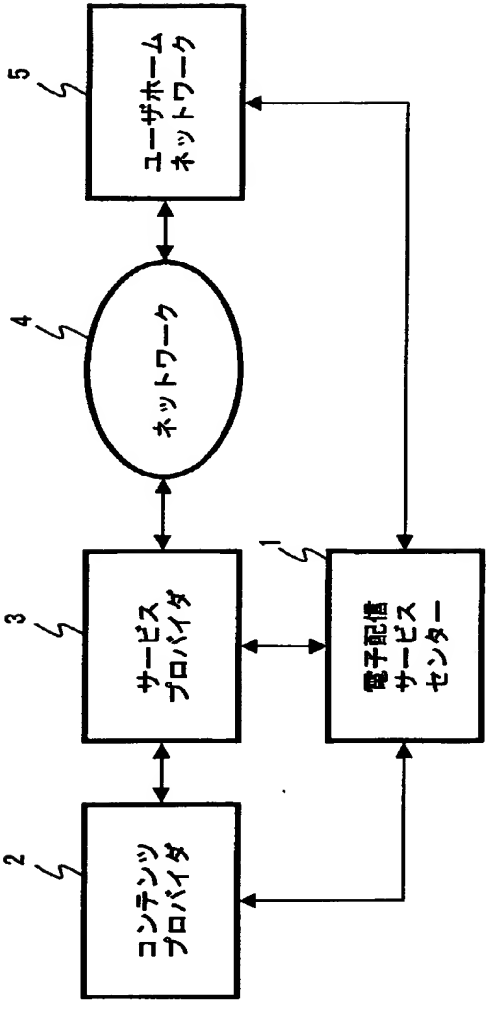


図１　電子音楽配信システムの全体構成

【図２】

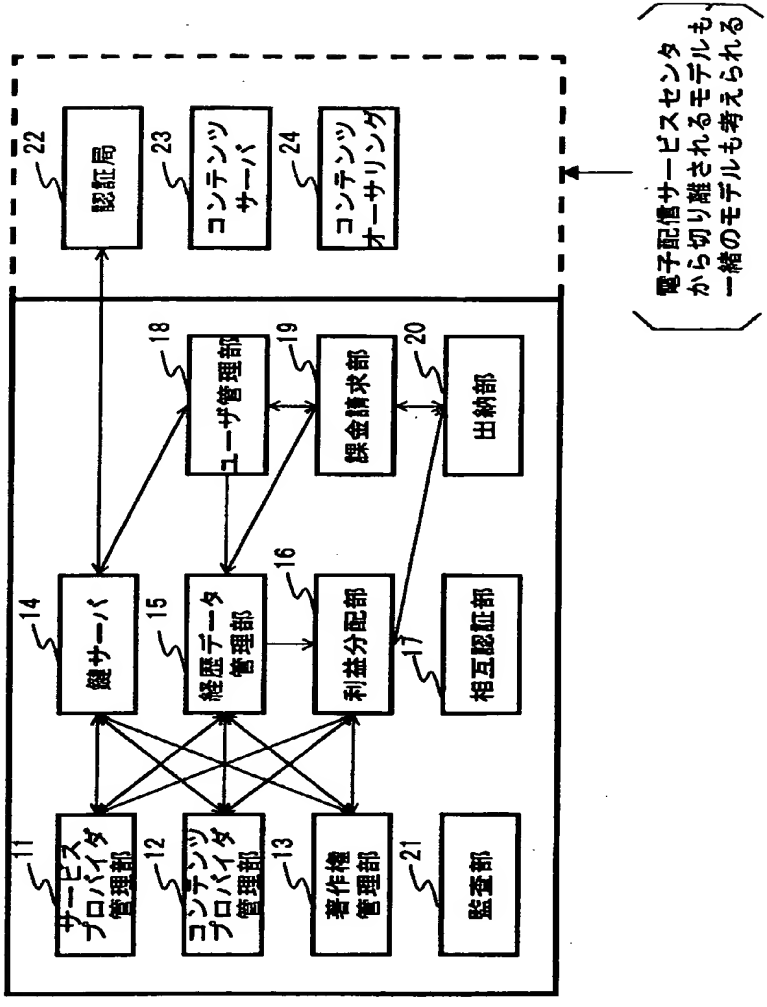


図２ 電子配信サービスセンタの構成

【図３】

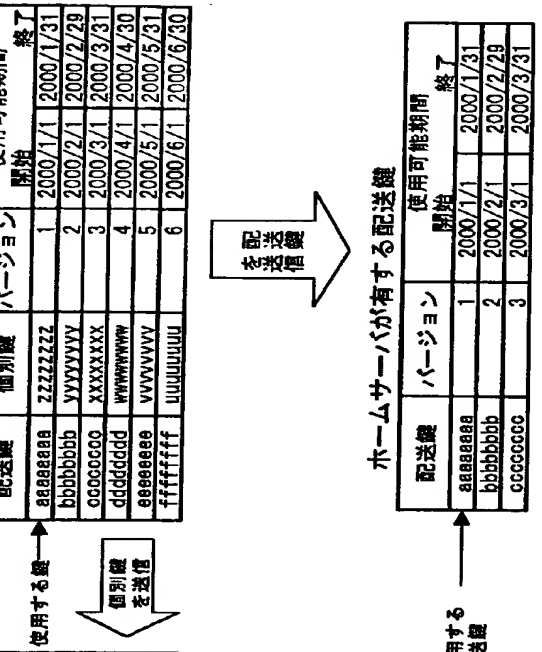


図３ 鍵の定期的な送信例（１）

【図４】

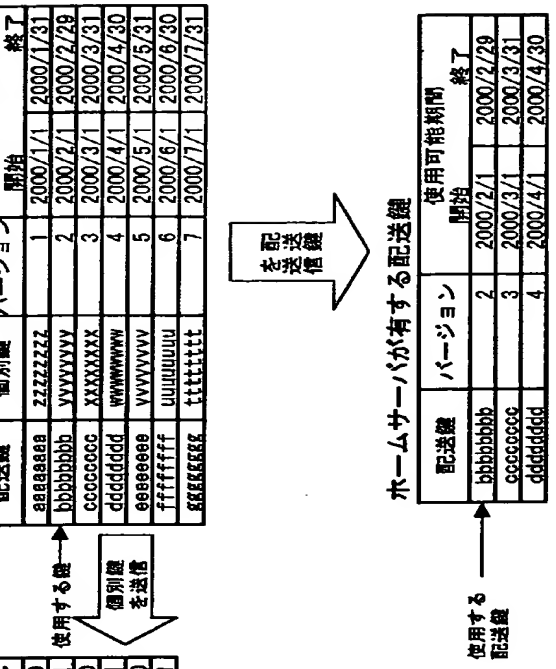


図４ 鍵の定期的な送信例（２）

【図５】

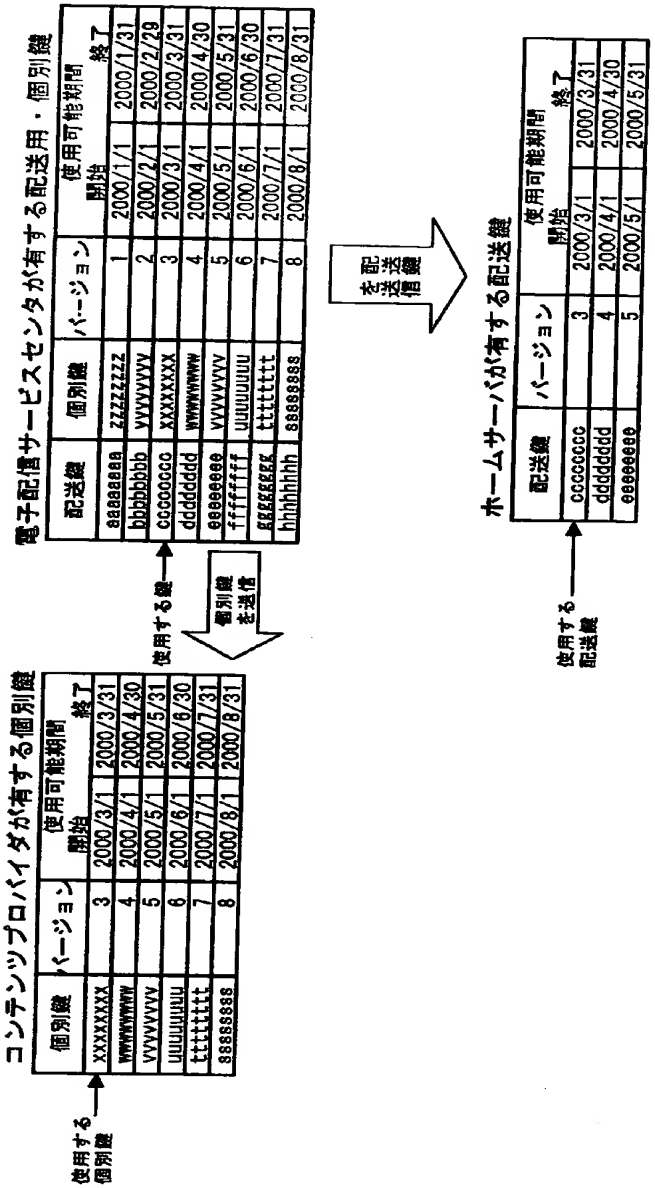


図５ 鍵の定期的な送信例（３）

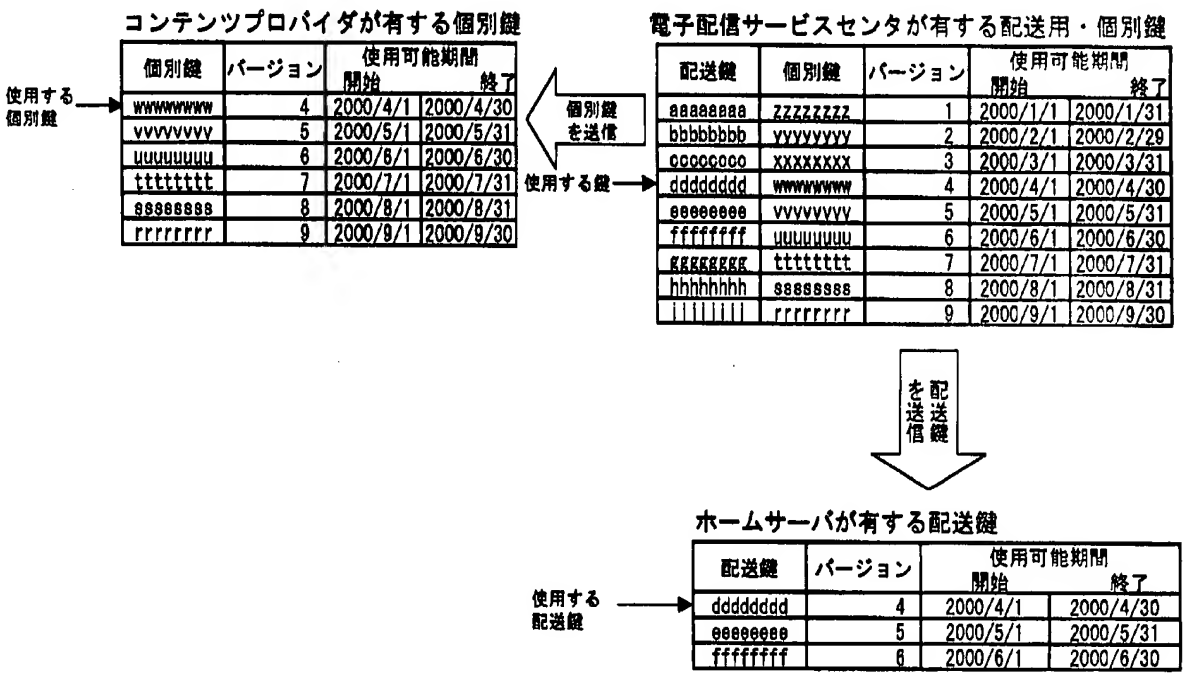
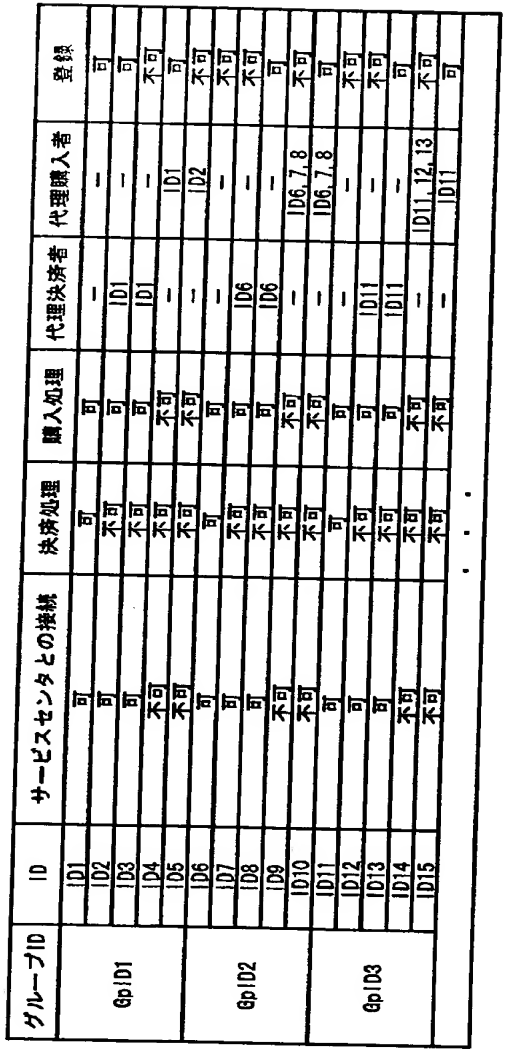


図６ 鍵の定期的な送信例（４）

出証特２０００－３０４９７２６

特平１１－２４２２９４

【図７】



グループID	ID	サービスセンタとの接続	決済処理	購入処理	代理決済者	代理購入者	登録
GpID1	ID1	可	可	可	—	—	可
	ID2	可	不可	可	ID1	—	可
	ID3	可	不可	可	ID1	—	不可
	ID4	不可	不可	不可	—	ID1	可
	ID5	不可	不可	不可	—	ID2	不可
GpID2	ID6	可	可	可	—	—	不可
	ID7	可	不可	可	ID6	—	不可
	ID8	可	不可	可	ID6	—	可
	ID9	不可	不可	不可	—	ID6,7,8	不可
	ID10	不可	不可	不可	—	ID6,7,8	可
GpID3	ID11	可	可	可	—	—	不可
	ID12	可	不可	可	ID11	—	不可
	ID13	可	不可	可	ID11	—	可
	ID14	不可	不可	不可	—	ID11,12,13	不可
	ID15	不可	不可	不可	—	ID11	可
			・・・				

図７ ユーザ登録データベース

【図８】

(A)

グループID	ＩＤ	サービスセンタとの接続	決済処理	決済ＩＤ	購入処理	代理決済者	代理購入者	登録	署名
GpID1	ID1	可	可	決済ＩＤ１	可	－	－	可	署名
	ID2	可	不可	－	可	ID1	－	可	
	ID3	可	不可	－	可	ID1	－	不可	
	ID4	不可	不可	－	不可	－	ID1	可	
	ID5	不可	不可	－	不可	－	ID2	不可	

(B)

グループID	ＩＤ	サービスセンタとの接続	決済処理	決済ＩＤ	購入処理	代理決済者	代理購入者	登録	署名
GpID2	ID6	可	可	決済ＩＤ２	可	－	－	可	署名
	ID7	可	不可	－	可	ID6	－	可	
	ID8	可	不可	－	可	ID6	－	不可	
	ID9	不可	不可	－	不可	－	ID6, 7, 8	可	
	ID10	不可	不可	－	不可	－	ID6, 7, 8	不可	

図８ グループの登録情報

【図９】

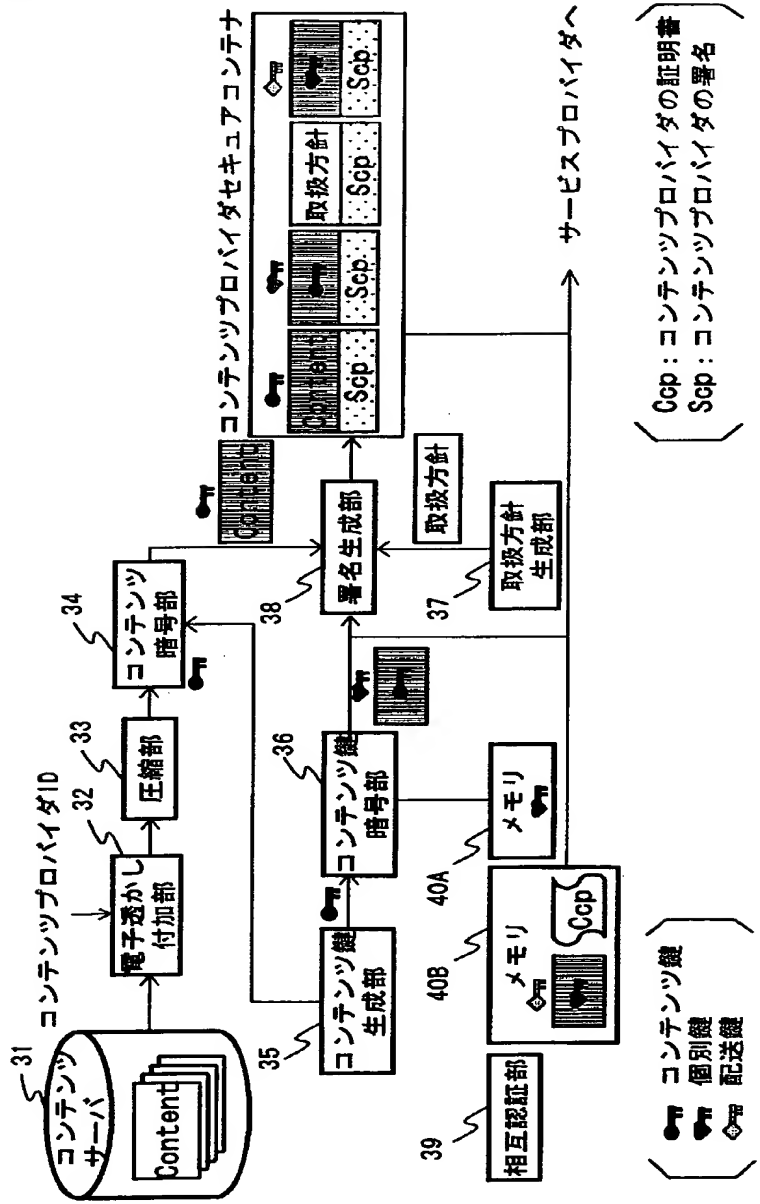


図９ コンテンツプロバイダの構成

【図１０】

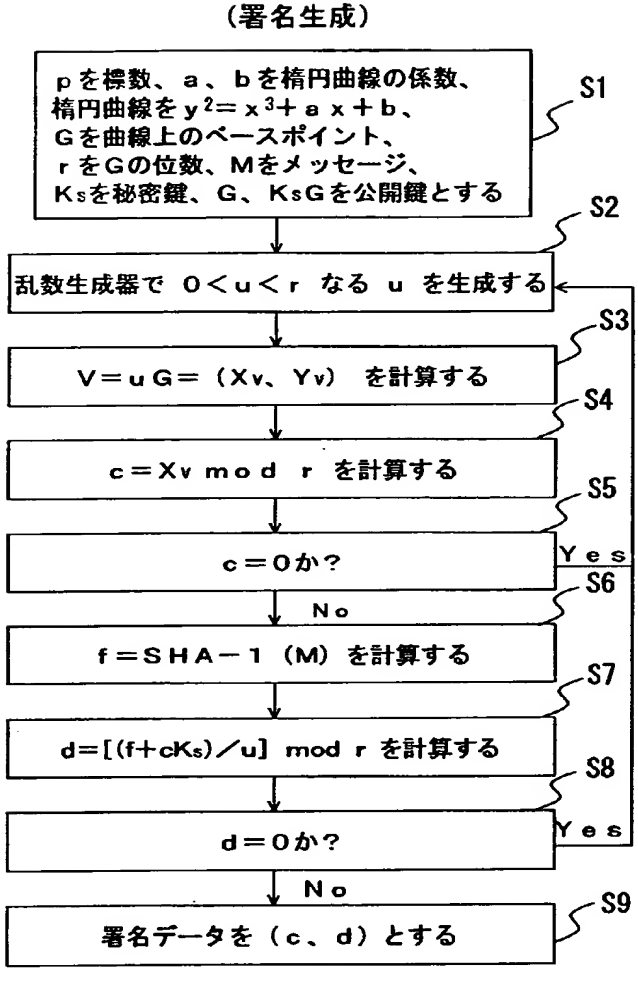


図１０　署名生成（IEEE P1363/D3)処理

【図１１】

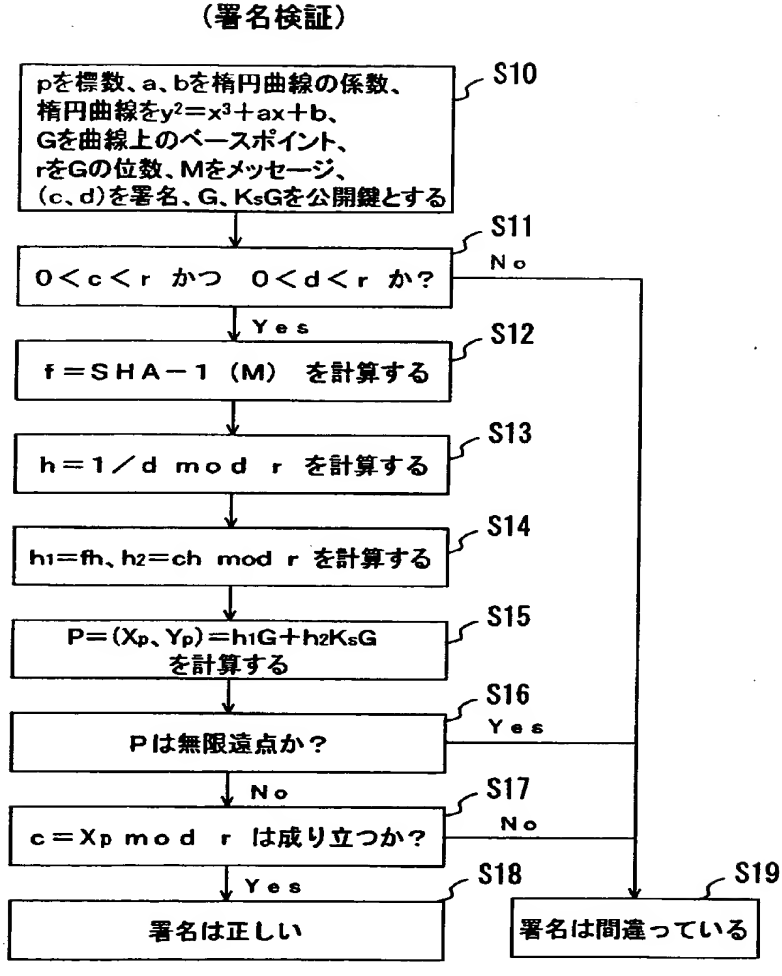


図１１　署名検証（IEEE P1363/D3）処理

【図１２】

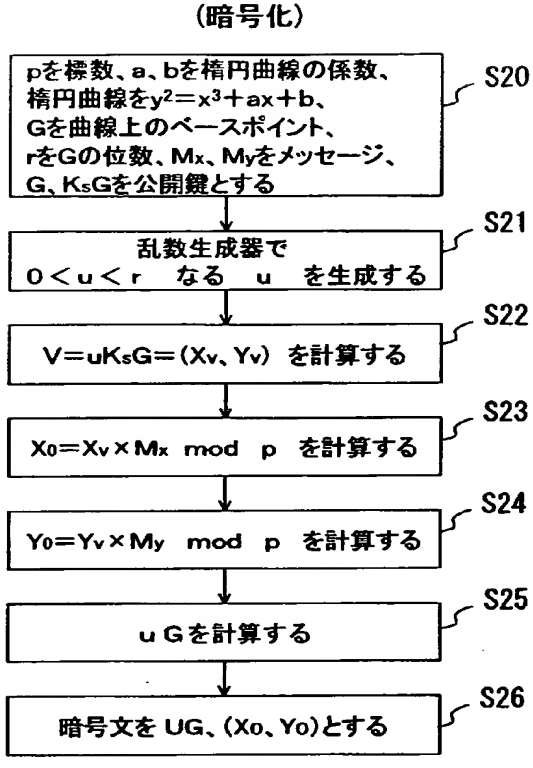


図１２　楕円曲線暗号を用いた暗号化（Menezes-Vanstone）処理

【図１３】

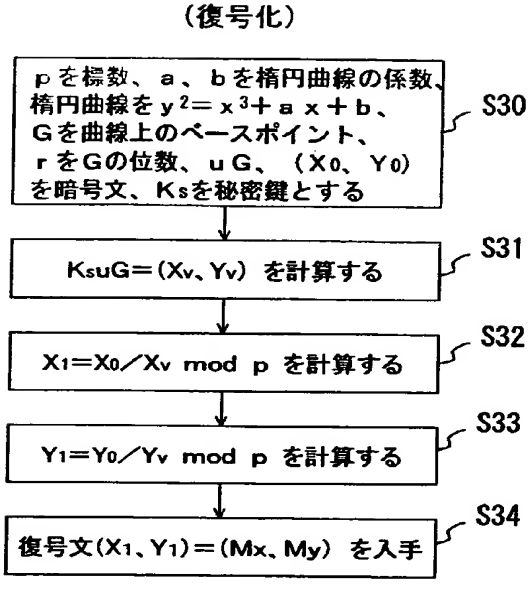


図１３　楕円曲線暗号を用いた復号化（Menezes-Vanstone）処理

【図１４】

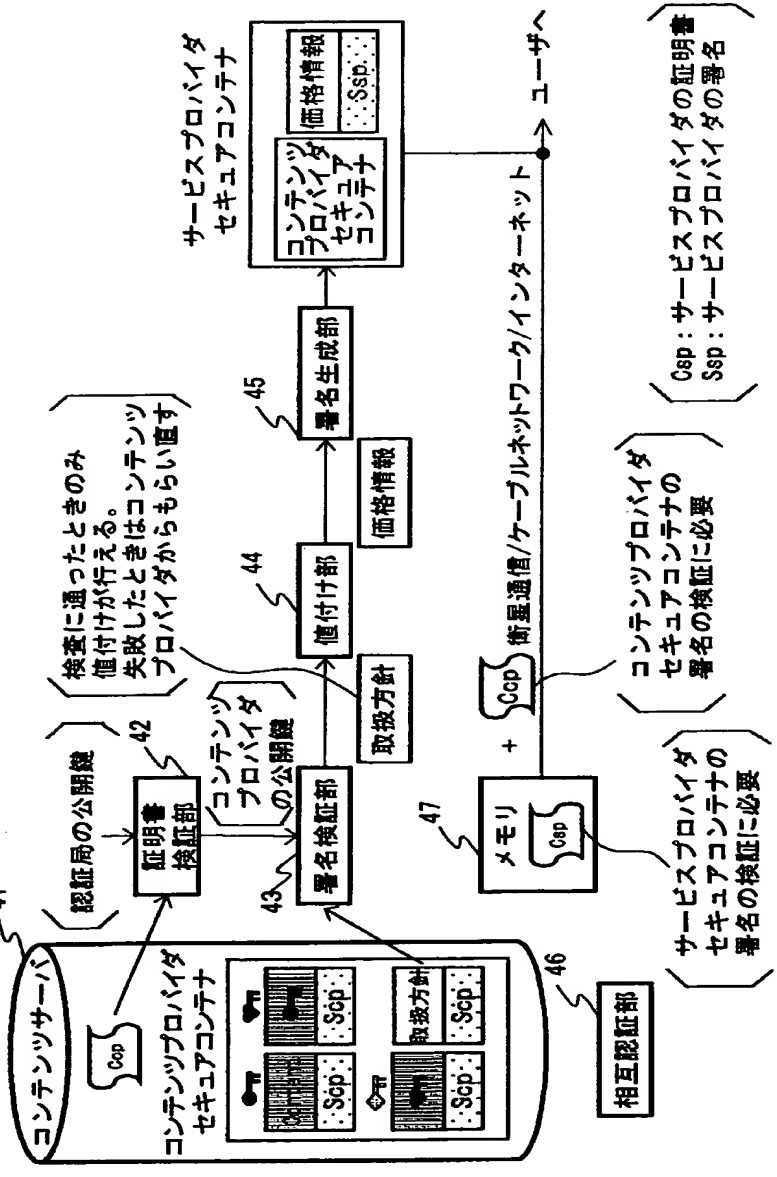


図１４　サービスプロバイダの構成

【図１５】

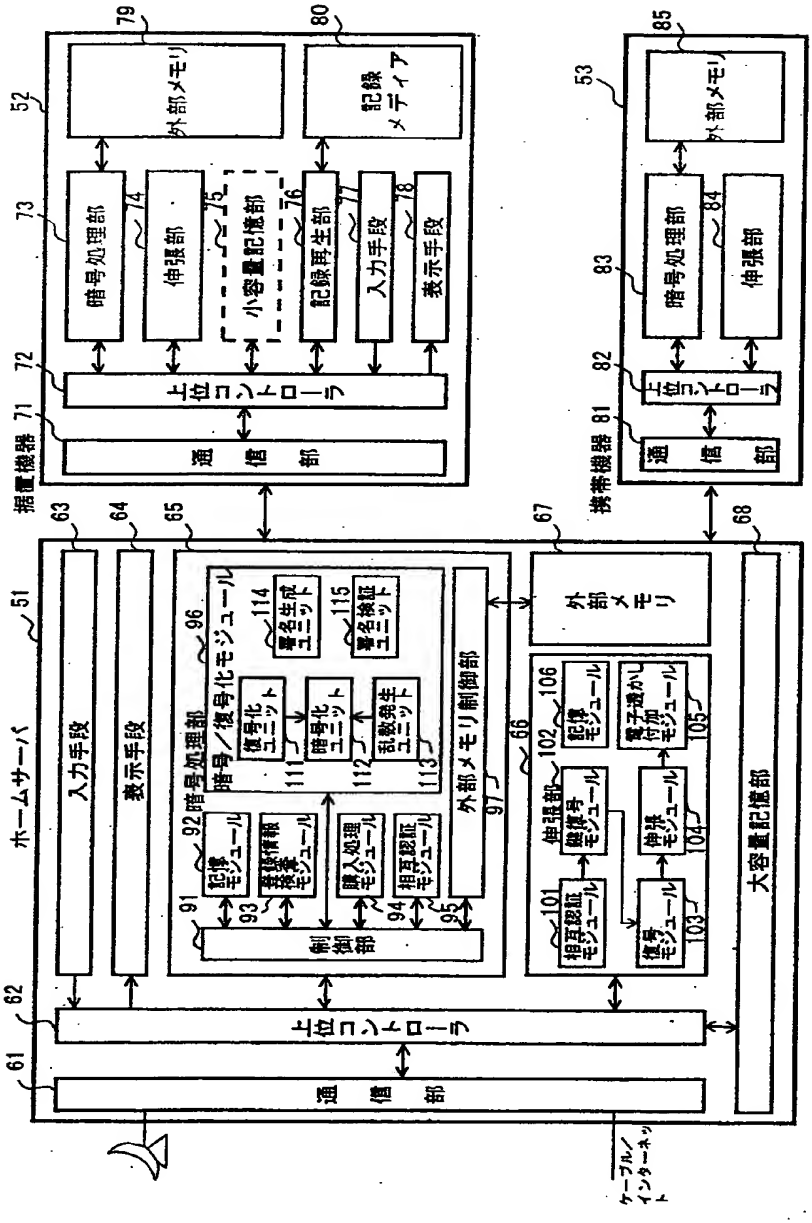


図１５　ユーザーホームネットワーク５

【図１６】

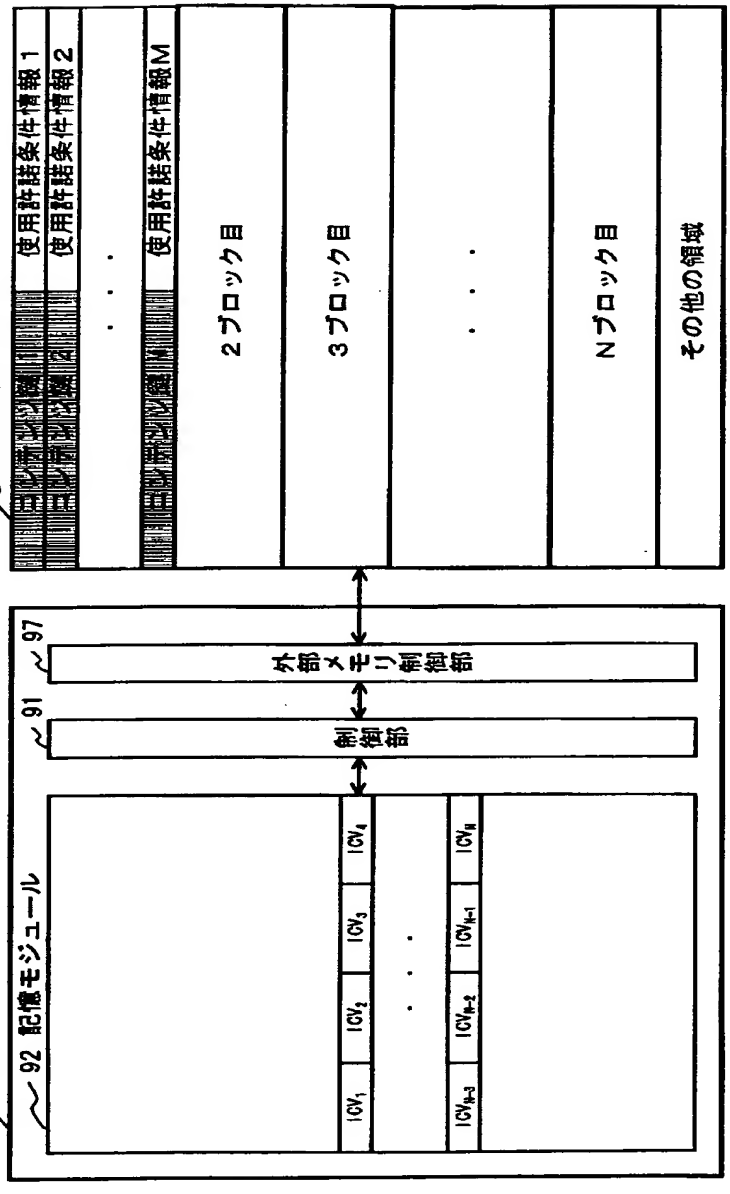


図１６　外部メモリ制御部の動作

【図１７】

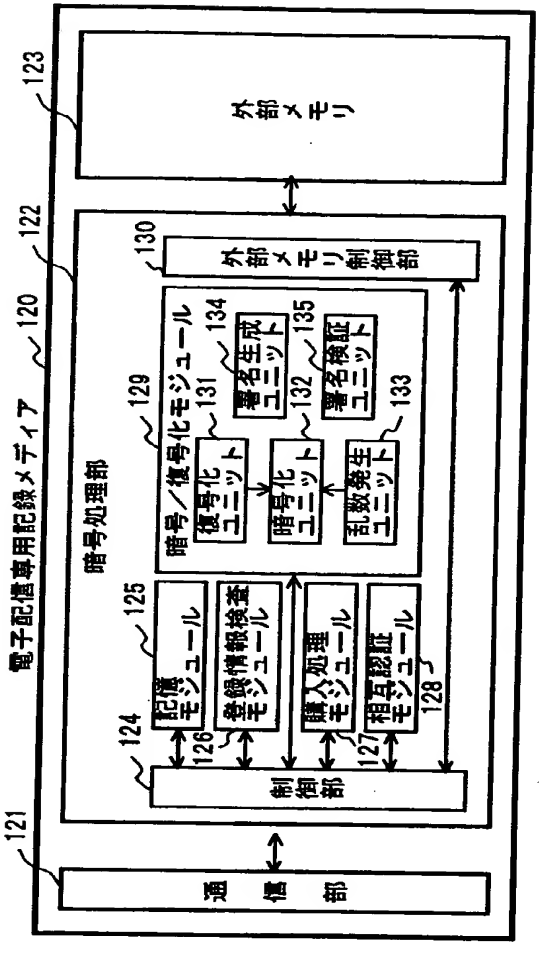


図１７　電子配信専用記録メディア

【図１８】

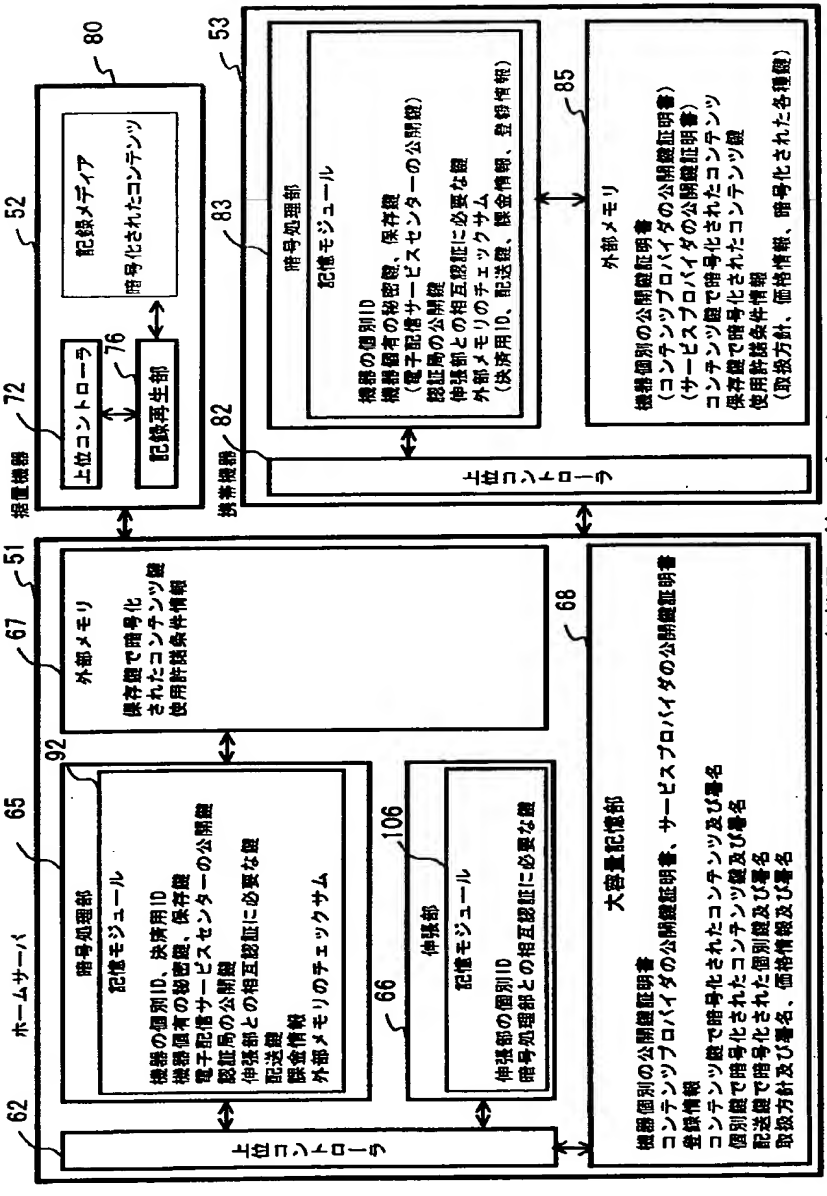


図１８　各機器の持つデータ

【図１９】

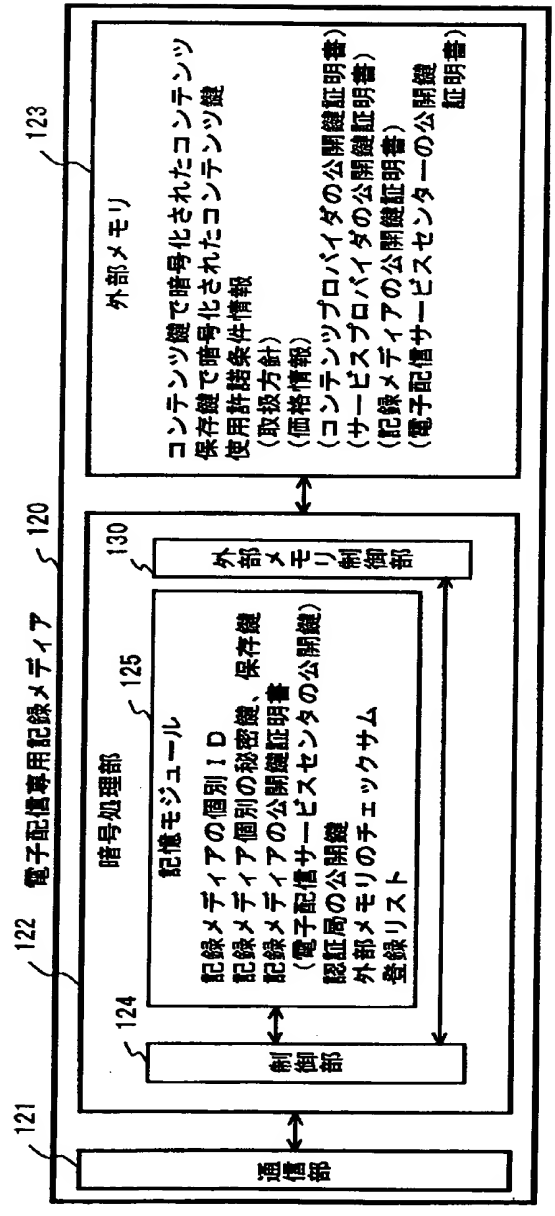


図１９　電子配信専用記録メディアの保持するデータ

【図２０】

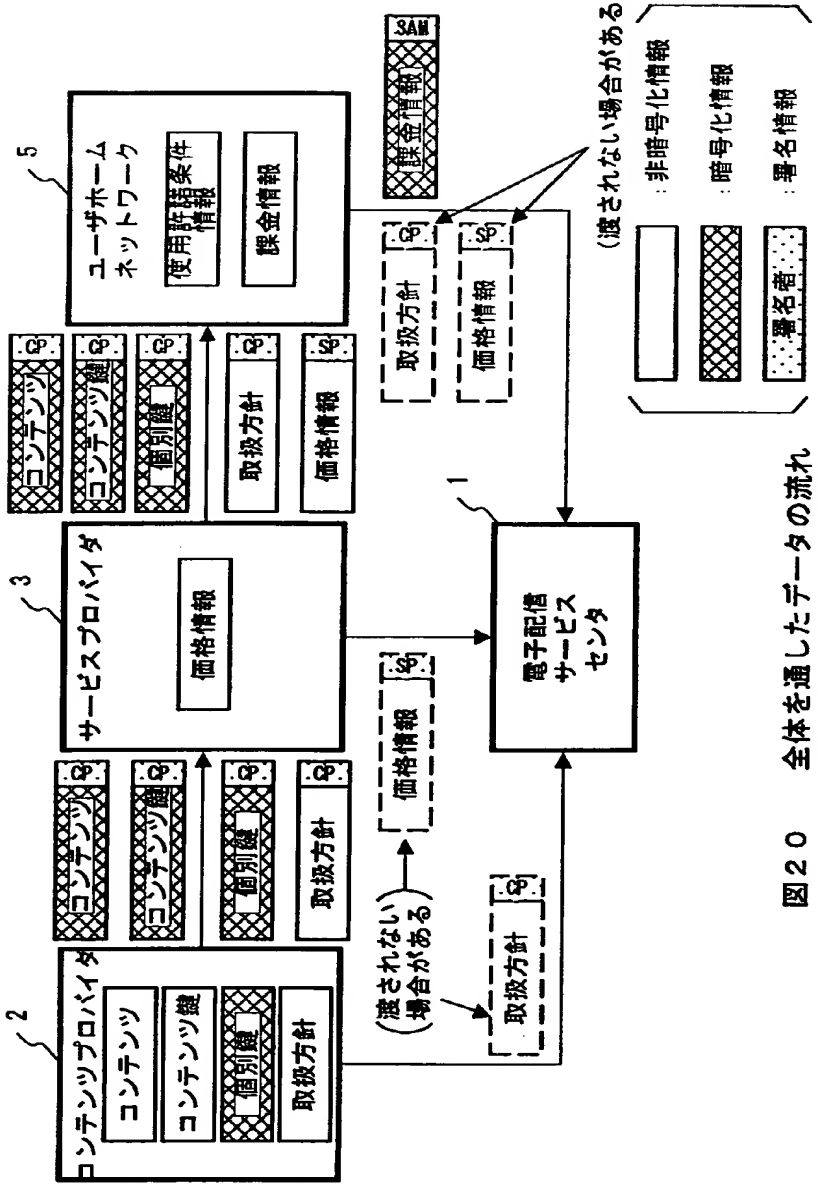


図２０　全体を通したデータの流れ

【図２１】

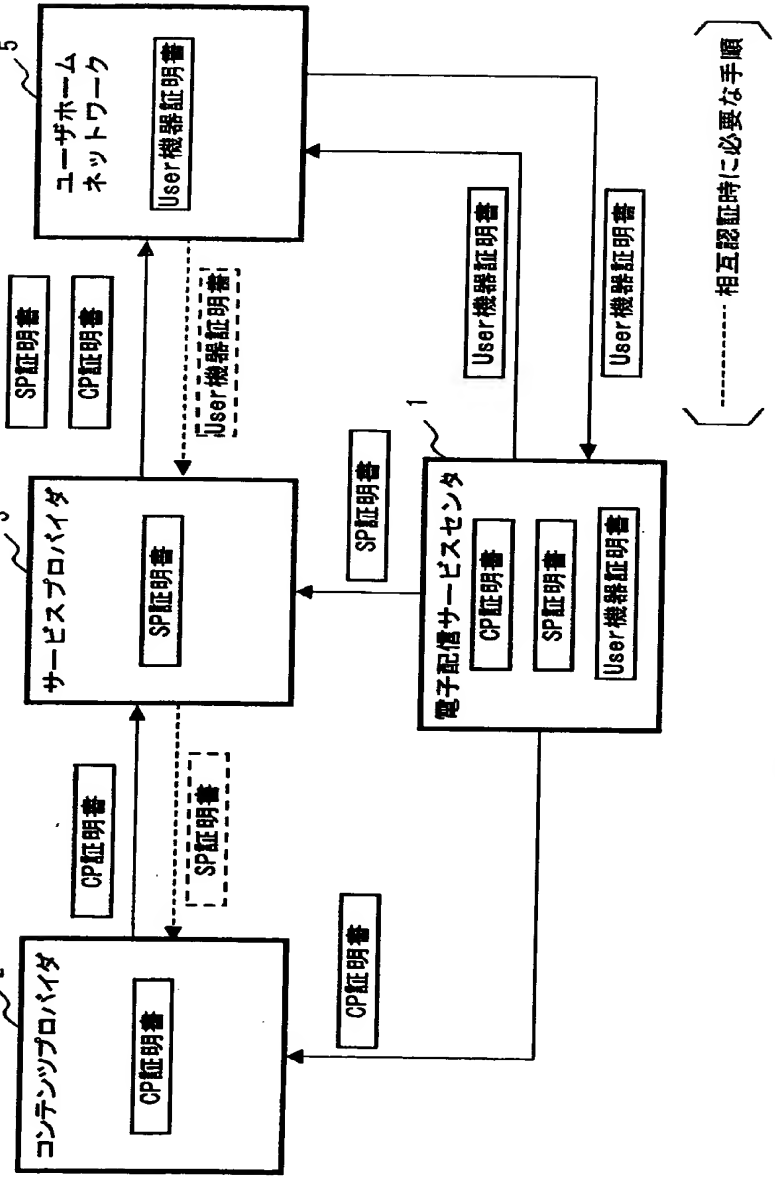


図２１　公開鍵証明書の流れ

【図２２】

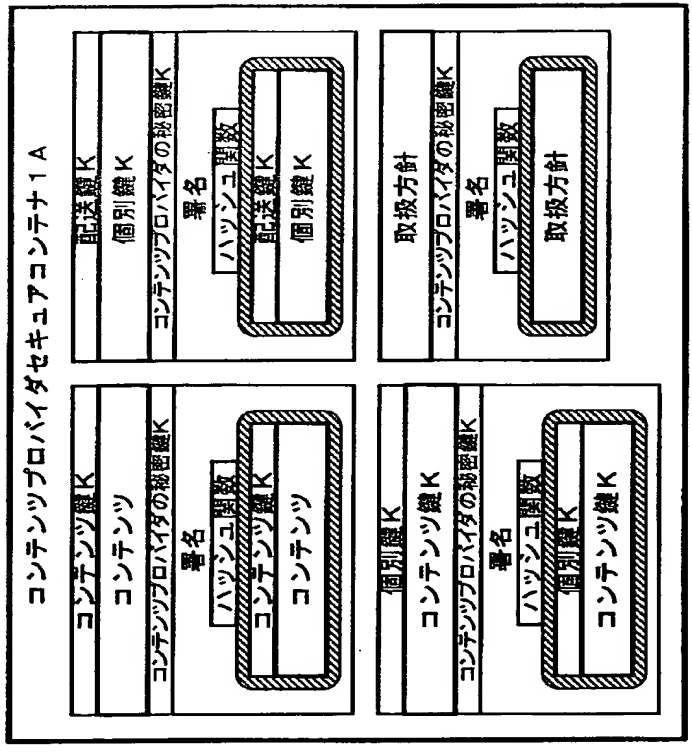


図２２　コンテンツプロバイダセキュアコンテナ

【図２３】

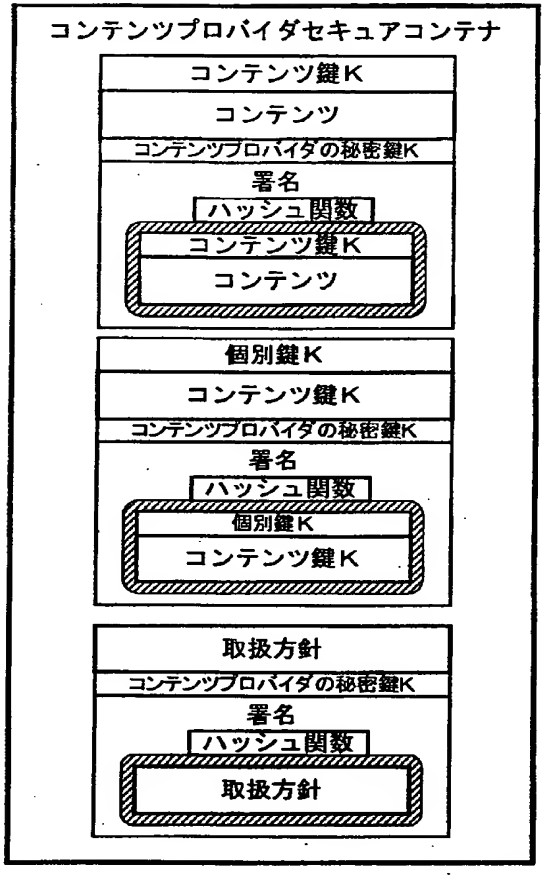


図２３　コンテンツプロバイダセキュアコンテナの他の例

【図２４】

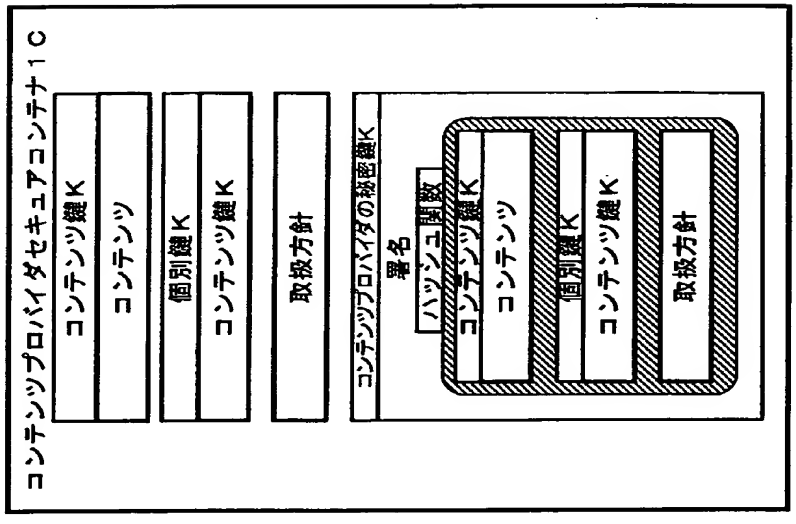


図２４　コンテンツプロバイダセキュアコンテナの他の例

【図２５】

図２５　コンテンツプロバイダセキュアコンテナの他の例

【図２６】

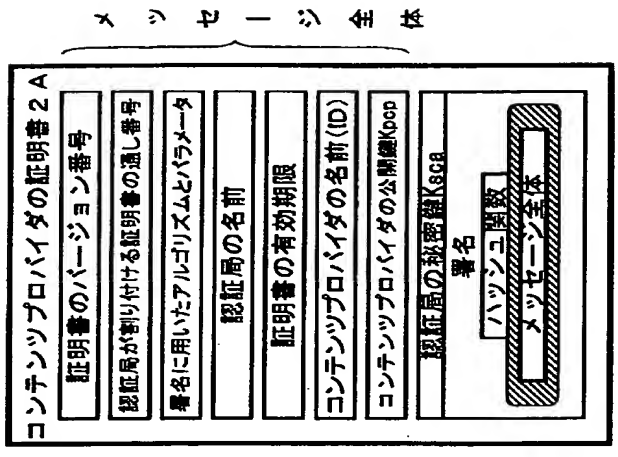


図２６　コンテンツプロバイダの公開鍵証明書

【図２７】

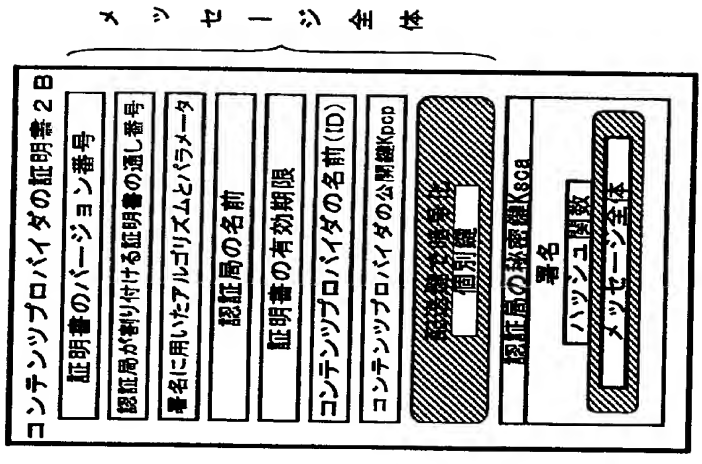


図２７　コンテンツプロバイダの公開鍵証明書の他の例

【図２８】

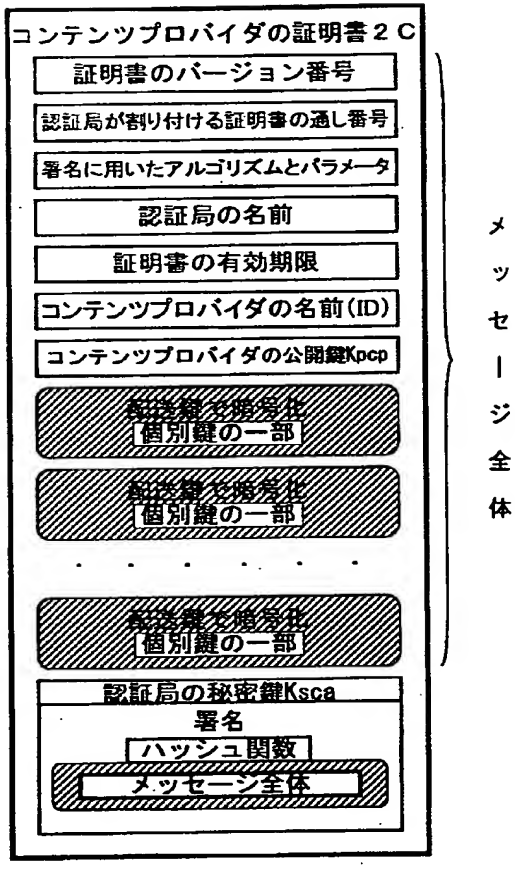


図２８　コンテンツプロバイダの公開鍵証明書の他の例

【図２９】

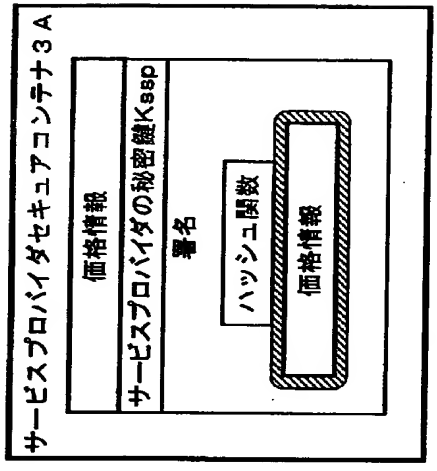


図２９　サービスプロバイダセキュアコンテナ

【図３０】

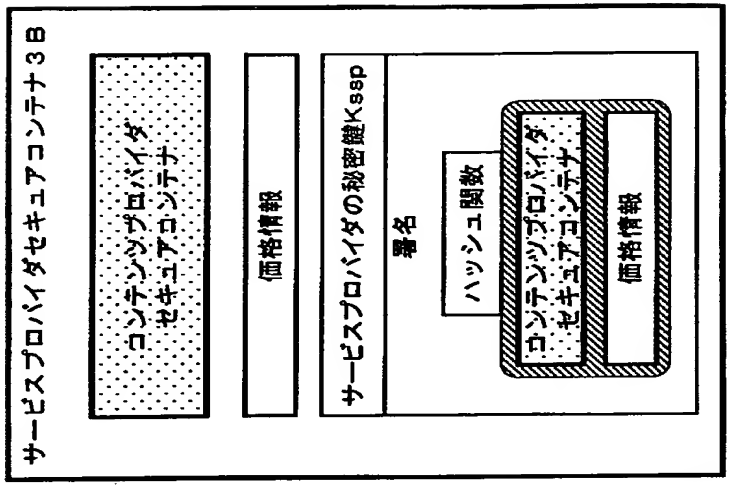


図３０　サービスプロバイダセキュアコンテナの他の例

【図３１】

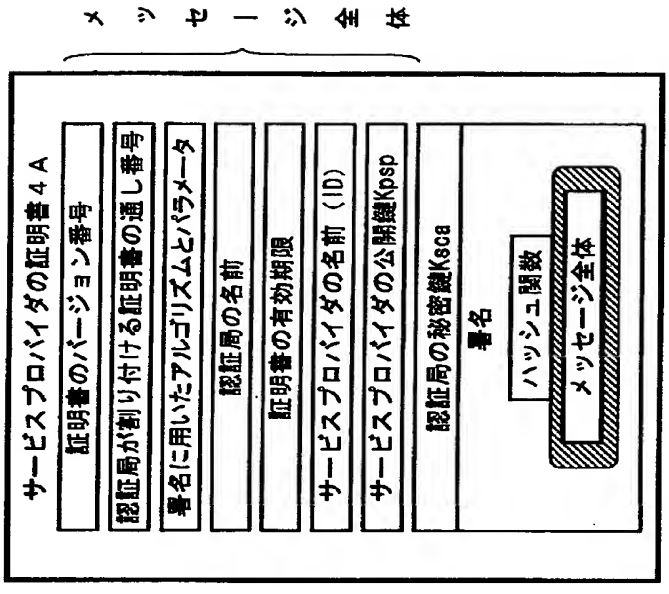


図３１　サービスプロバイダの公開鍵証明書

【図３２】

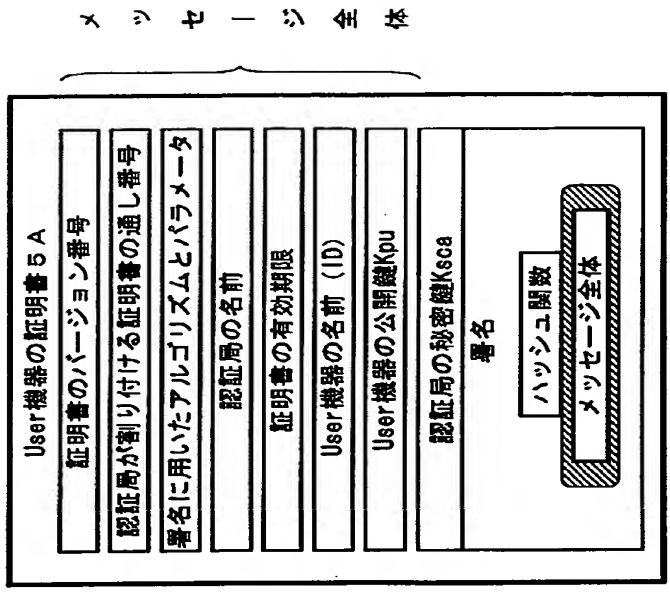


図３２　User機器の公開鍵証明書

【図３３】

データの種別	
取扱方針の種類（シングル）	
取扱方針の有効期限	
コンテンツのＩＤ	
コンテンツプロバイダのＩＤ	
取扱方針のＩＤ	
取扱方針のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのＩＤ	
世代管理情報	
ルールの数	
ルールのアドレス情報	
ルール1	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
・・・	・・・
ルールN	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
（署名の検証の有無）	
公開鍵証明書	
署名	

図３３　シングルコンテンツの取扱方針

【図３４】

データの種別	
取扱方針の種類（アルバム）	
取扱方針の有効期限	
アルバムのＩＤ	
取扱方針のバージョン	
コンテンツプロバイダのＩＤ	
取扱方針のＩＤ	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのＩＤ	
シングルコンテンツの取扱方針の数	
シングルコンテンツの取扱方針のアドレス情報	
シングル	取扱方針１
	⋮
	取扱方針Ｎ
世代管理情報	
ルールの数	
ルールのアドレス情報	
ルール１	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
⋮	⋮
ルールＮ	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図３４　アルバムコンテンツの取扱方針

【図３５】

データの種別	
取扱方針の種類（シングル）	
取扱方針の有効期限	
コンテンツのＩＤ	
コンテンツプロバイダのＩＤ	
取扱方針のＩＤ	
取扱方針のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのＩＤ	
世代管理情報	
ルールの数	
ルールのアドレス情報	
ルール１	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	データサイズ
	送信情報
・・・	・・・
ルールＮ	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図３５　シングルコンテンツの取扱方針のその他の例

【図３６】

データの種別	
取扱方針の種類（アルバム）	
取扱方針の有効期限	
アルバムのＩＤ	
取扱方針のバージョン	
コンテンツプロバイダのＩＤ	
取扱方針のＩＤ	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのＩＤ	
シングルコンテンツの取扱方針の数	
シングルコンテンツの取扱方針のアドレス情報	
シングル	取扱方針１
	・・・
	取扱方針Ｎ
世代管理情報	
ルールの数	
ルールのアドレス情報	
ルール１	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	データサイズ
	送信情報
・・・	・・・
ルールＮ	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図３６　アルバムコンテンツの取扱方針のその他の例

【図３７】

データの種別	
価格情報の種類（シングル）	
価格情報の有効期限	
コンテンツのＩＤ	
サービスプロバイダのＩＤ	
価格情報のＩＤ	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのＩＤ	
取扱方針のＩＤ	
ルールの数	
ルールのアドレス情報	
ルール1	ルール番号（Rule#）
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
・・・	・・・
ルールN	ルール番号（Rule#）
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図３７　シングルコンテンツの価格情報

【図３８】

データの種別		
価格情報の種類（アルバム）		
価格情報の有効期限		
アルバムのＩＤ		
サービスプロバイダのＩＤ		
価格情報のＩＤ		
価格情報のバージョン		
地域コード		
使用可能機器条件		
使用可能User条件		
コンテンツプロバイダのＩＤ		
取扱方針のＩＤ		
シングルコンテンツの価格情報の数		
シングルコンテンツの価格情報のアドレス情報		
シングル	価格情報１	
	：	
	価格情報Ｎ	
ルールの数		
ルールのアドレス情報		
ルール１	ルール番号（Rule#）	
	サービスプロバイダの利益額	
	サービスプロバイダの利益率	
	価格	
	データサイズ	
	送信情報	
：	：	
ルールＮ	ルール番号（Rule#）	
	サービスプロバイダの利益額	
	サービスプロバイダの利益率	
	価格	
	データサイズ	
	送信情報	
（署名の検出の有無）		
公開鍵証明書		
署名		

図３８　アルバムコンテンツの価格情報

【図３９】

データの種別	
価格情報の種類（シングル）	
価格情報の有効期限	
コンテンツのＩＤ	
サービスプロバイダのＩＤ	
価格情報のＩＤ	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのＩＤ	
取扱方針のＩＤ	
ルールの数	
ルールのアドレス情報	
ルール1	ルール番号（Rule#）
	価格
	データサイズ
	送信情報
・・・	・・・
ルールN	ルール番号（Rule#）
	価格
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図３９　シングルコンテンツの価格情報の他の例

【図４０】

データの種別	
価格情報の種類（アルバム）	
価格情報の有効期限	
アルバムのＩＤ	
サービスプロバイダのＩＤ	
価格情報のＩＤ	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのＩＤ	
取扱方針のＩＤ	
シングルコンテンツの価格情報の数	
シングルコンテンツの価格情報のアドレス情報	
シングル	価格情報１
	・・・
	価格情報Ｎ
ルールの数	
ルールのアドレス情報	
ルール１	ルール番号（Rule#）
	価格
	データサイズ
	送信情報
・・・	・・・
ルールＮ	ルール番号（Rule#）
	価格
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図４０　アルバムコンテンツの価格情報の他の例

【図４１】

データの種別
使用許諾条件情報の種類
使用許諾条件情報の有効期限
コンテンツのＩＤ
アルバムのＩＤ
暗号処理部のＩＤ
ユーザのＩＤ
コンテンツプロバイダのＩＤ
取扱方針のＩＤ
取扱方針のバージョン
サービスプロバイダのＩＤ
価格情報のＩＤ
価格情報のバージョン
使用許諾条件情報のＩＤ
再生権（利用権）のルール番号
利用権内容番号
再生残り回数
再生権の有効期限
複製権（利用権）のルール番号
利用権内容番号
複製残り回数
世代管理情報
再生権を保有する暗号処理部のＩＤ

図４１　使用許諾条件情報

【図４２】

データの種別
暗号処理部のＩＤ
ユーザのＩＤ
コンテンツのＩＤ
コンテンツプロバイダのＩＤ
取扱方針のＩＤ
取扱方針のバージョン
サービスプロバイダのＩＤ
価格情報のＩＤ
価格情報のバージョン
使用許諾条件のＩＤ
ルール番号（Rule#）
コンテンツプロバイダの利益額／利益率
サービスプロバイダの利益額／利益率
世代管理情報
コンテンツプロバイダの設定した送信情報のデータサイズ
コンテンツプロバイダの設定した送信情報
サービスプロバイダの設定した送信情報のデータサイズ
サービスプロバイダの設定した送信情報
供給元のＩＤ

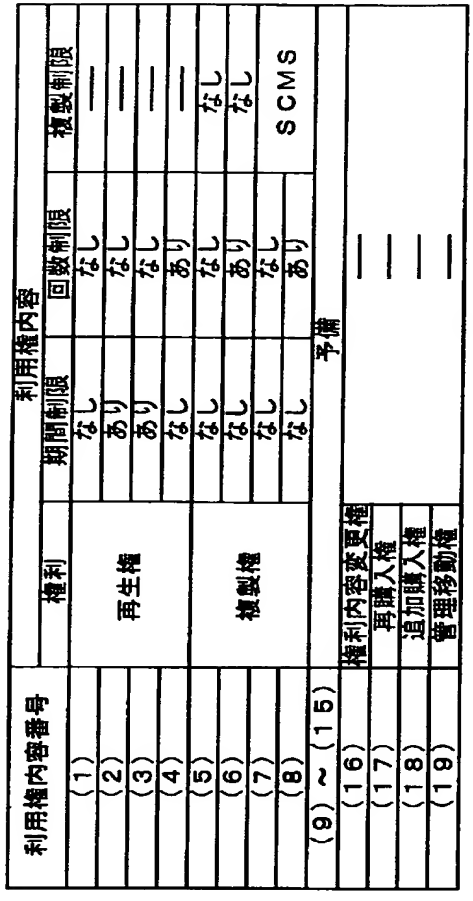
図４２　課金情報

【図４３】

データの種別
暗号処理部のＩＤ
ユーザのＩＤ
コンテンツのＩＤ
コンテンツプロバイダのＩＤ
取扱方針のＩＤ
取扱方針のバージョン
サービスプロバイダのＩＤ
価格情報のＩＤ
価格情報のバージョン
使用許諾条件のＩＤ
ルール番号（Rule#）
世代管理情報
コンテンツプロバイダの設定した送信情報のデータサイズ
コンテンツプロバイダの設定した送信情報
サービスプロバイダの設定した送信情報のデータサイズ
サービスプロバイダの設定した送信情報
供給元のＩＤ

図４３　課金情報の他の例

【図４４】



利用権内容番号	利用権内容			
	権利	期間制限	回数制限	複製制限
（１）	再生権	なし	なし	―
（２）		あり	なし	―
（３）		あり	なし	―
（４）		なし	あり	―
（５）	複製権	なし	なし	なし
（６）		なし	あり	なし
（７）		なし	なし	SCMS
（８）		なし	あり	
（９）～（１５）	予備			
（１６）	権利内容変更権	―	―	―
（１７）	再購入権			
（１８）	追加購入権			
（１９）	管理移動権			

図４４　利用権内容の一覧

【図４５】

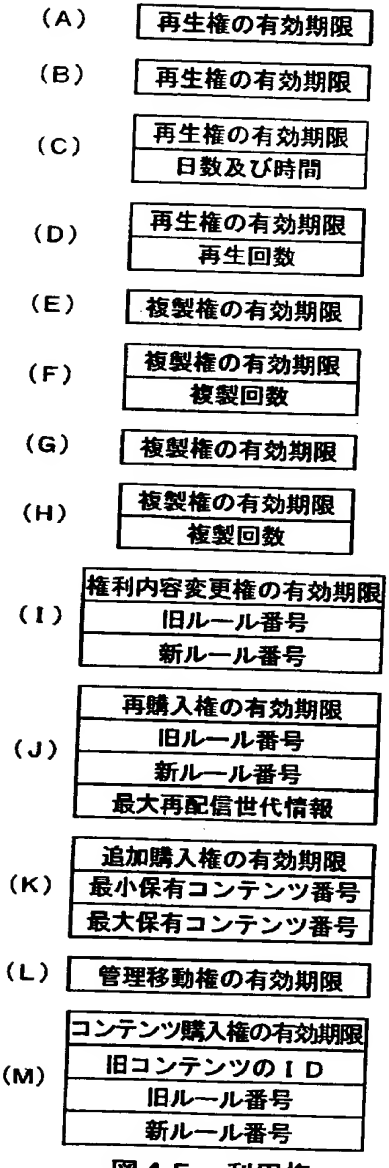

(A)
再生権の有効期限
(B)
再生権の有効期限
(C)
再生権の有効期限
日数及び時間
(D)
再生権の有効期限
再生回数
(E)
複製権の有効期限
(F)
複製権の有効期限
複製回数
(G)
複製権の有効期限
(H)
複製権の有効期限
複製回数
(I)
権利内容変更権の有効期限
旧ルール番号
新ルール番号
(J)
再購入権の有効期限
旧ルール番号
新ルール番号
最大再配信世代情報
(K)
追加購入権の有効期限
最小保有コンテンツ番号
最大保有コンテンツ番号
(L)
管理移動権の有効期限
(M)
コンテンツ購入権の有効期限
旧コンテンツのＩＤ
旧ルール番号
新ルール番号

図４５　利用権

【図４６】

データの種別
コンテンツの種類（シングル）
コンテンツの有効期限
コンテンツのカテゴリー
コンテンツのＩＤ
コンテンツプロバイダのＩＤ
コンテンツの暗号方式
暗号化したコンテンツのデータ長
暗号化したコンテンツ
公開鍵証明書
署名

図４６　シングルコンテンツ

【図４７】

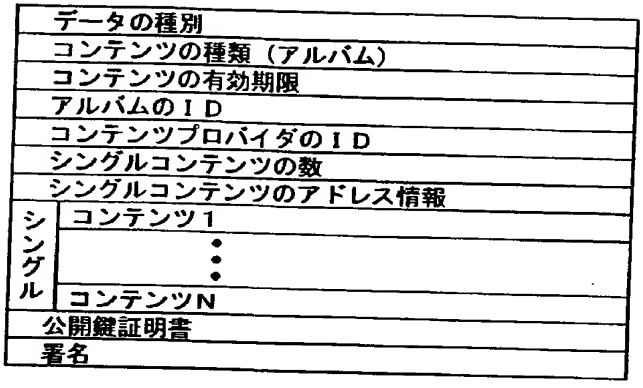


図４７　アルバムコンテンツ

【図４８】

データの種別
鍵データの種類（シングル）
鍵の有効期限
コンテンツのＩＤ
コンテンツプロバイダのＩＤ
鍵のバージョン
コンテンツ鍵の暗号方式
暗号化したコンテンツ鍵
個別鍵の暗号方式
暗号化した個別鍵
公開鍵証明書
署名

図４８　シングルコンテンツ用の鍵データ

【図４９】

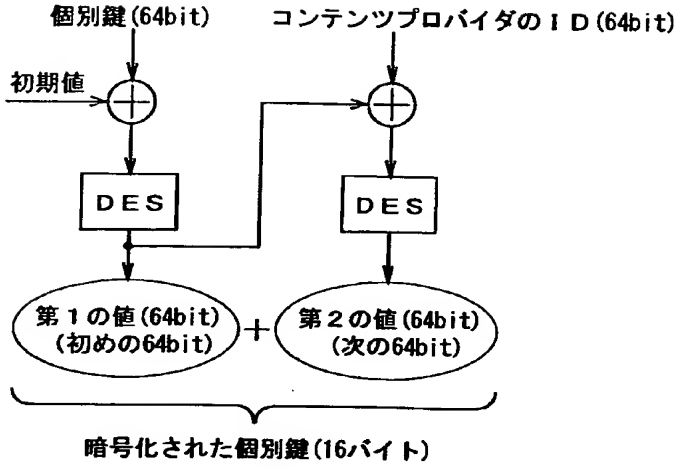


図４９　個別鍵の暗号化処理（Triple-DES-CBC）

【図５０】

	データの種別
	鍵データの種類（アルバム）
	鍵の有効期限
	アルバムのＩＤ
	コンテンツプロバイダＩＤ
	鍵のバージョン
	シングルコンテンツ用の鍵データの数
	シングルコンテンツ用の鍵データのアドレス情報
シングル	鍵データ１
	⋮
	鍵データＮ
	公開鍵証明書
	署名

図５０　アルバムコンテンツ用の鍵データ

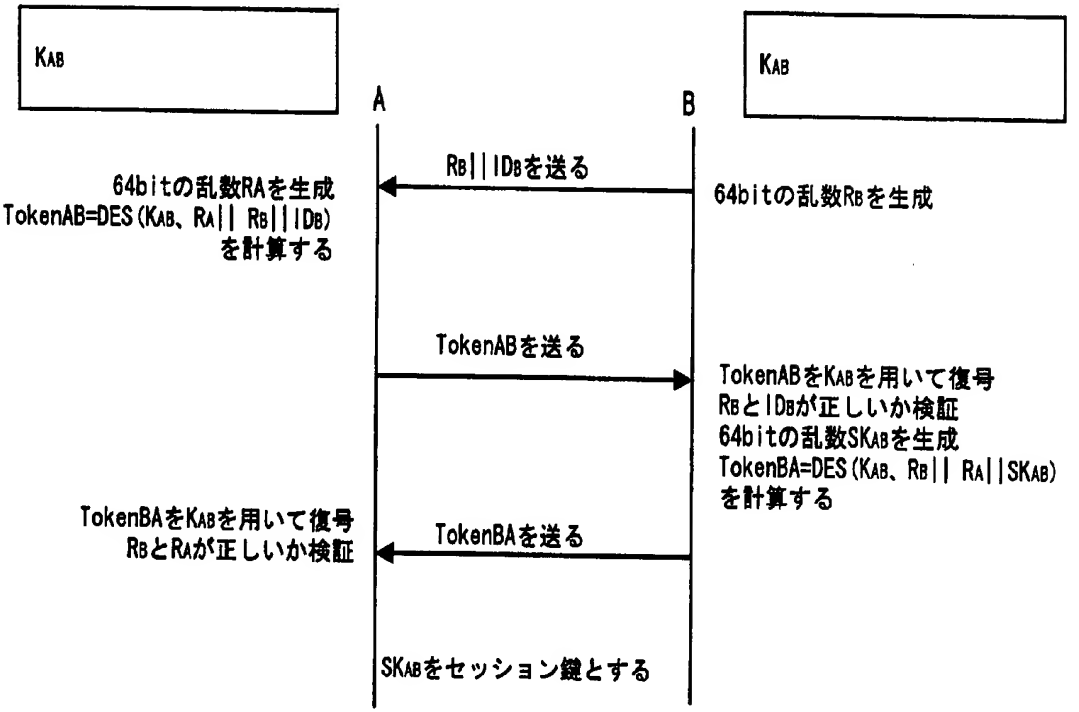


図５１　対称鍵暗号技術を用いた相互認証（ISO/IEC 9798-2）

出証特２０００－３０４９７２６

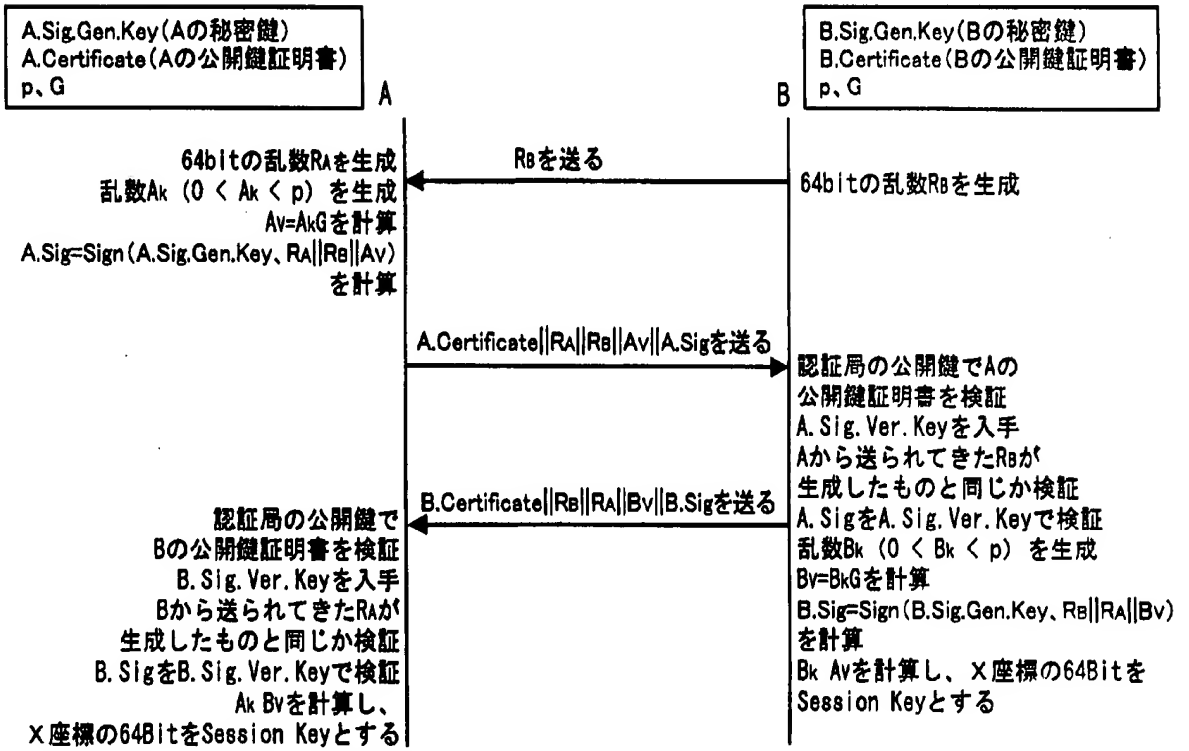


図５２　非対称鍵暗号技術を用いた相互認証（ISO/IEC 9798-3）

出証特２０００－３０４９７２６

特平１１－２４２２９４

【図５３】

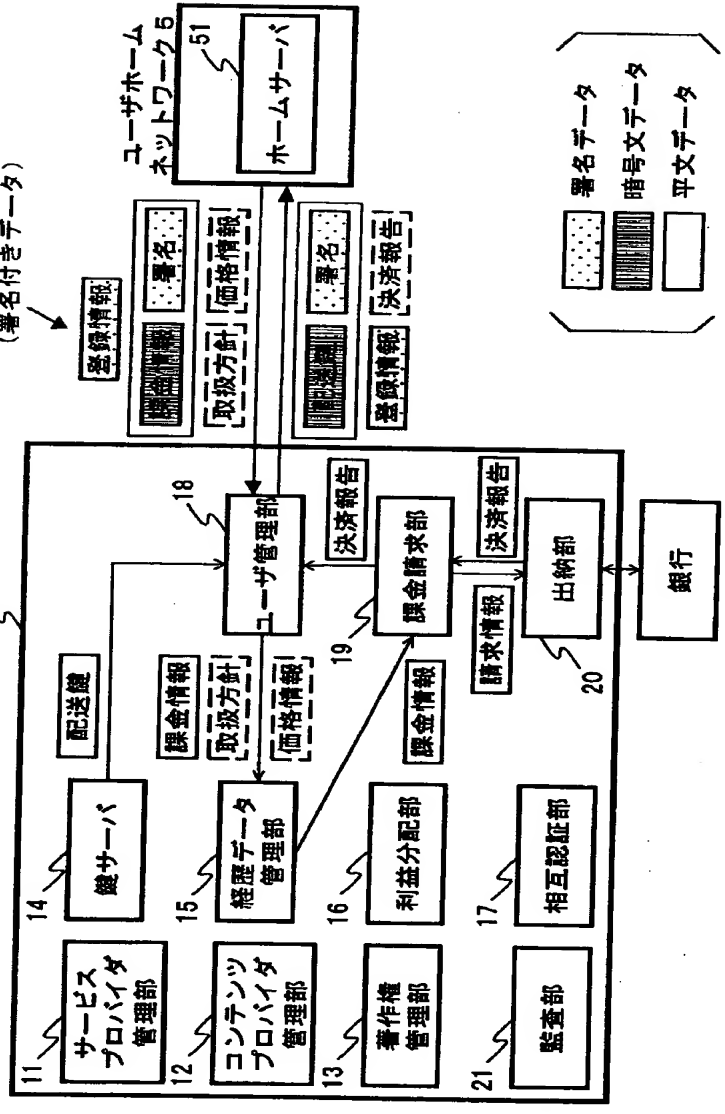


図５３　課金情報の送信動作

【図５４】

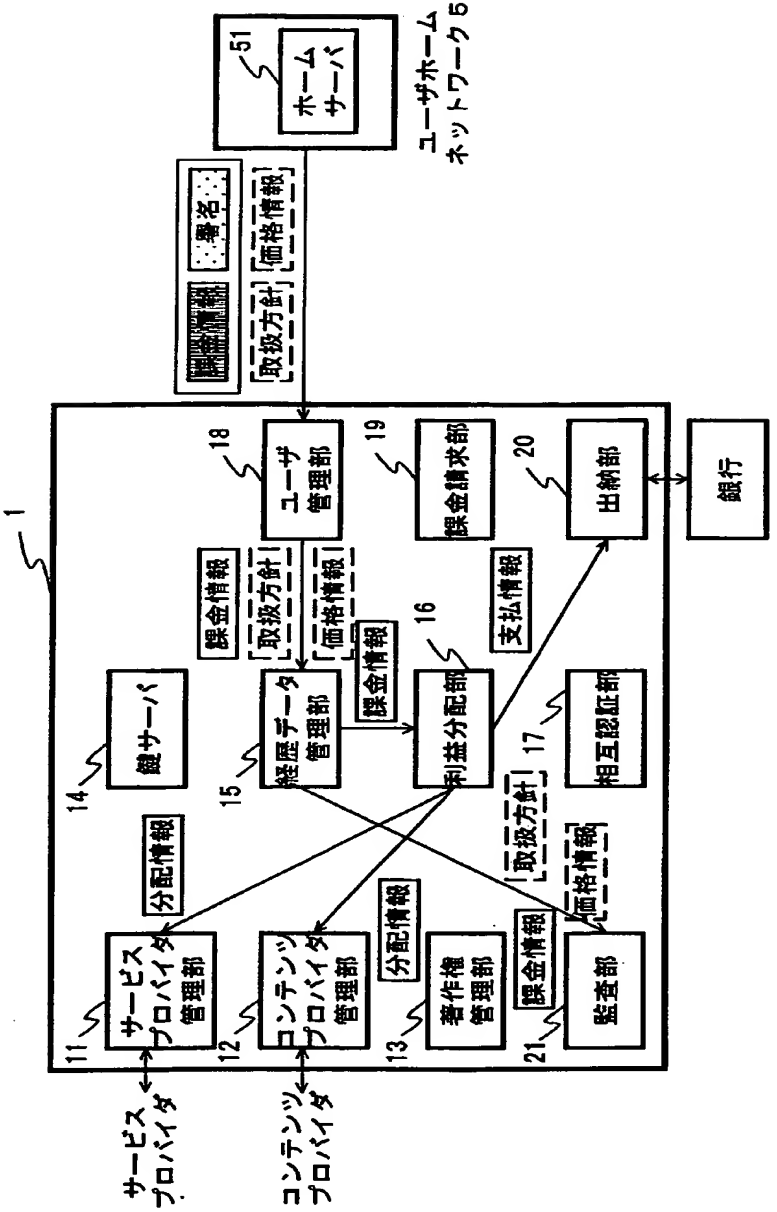


図５４　利益分配処理動作

【図５５】

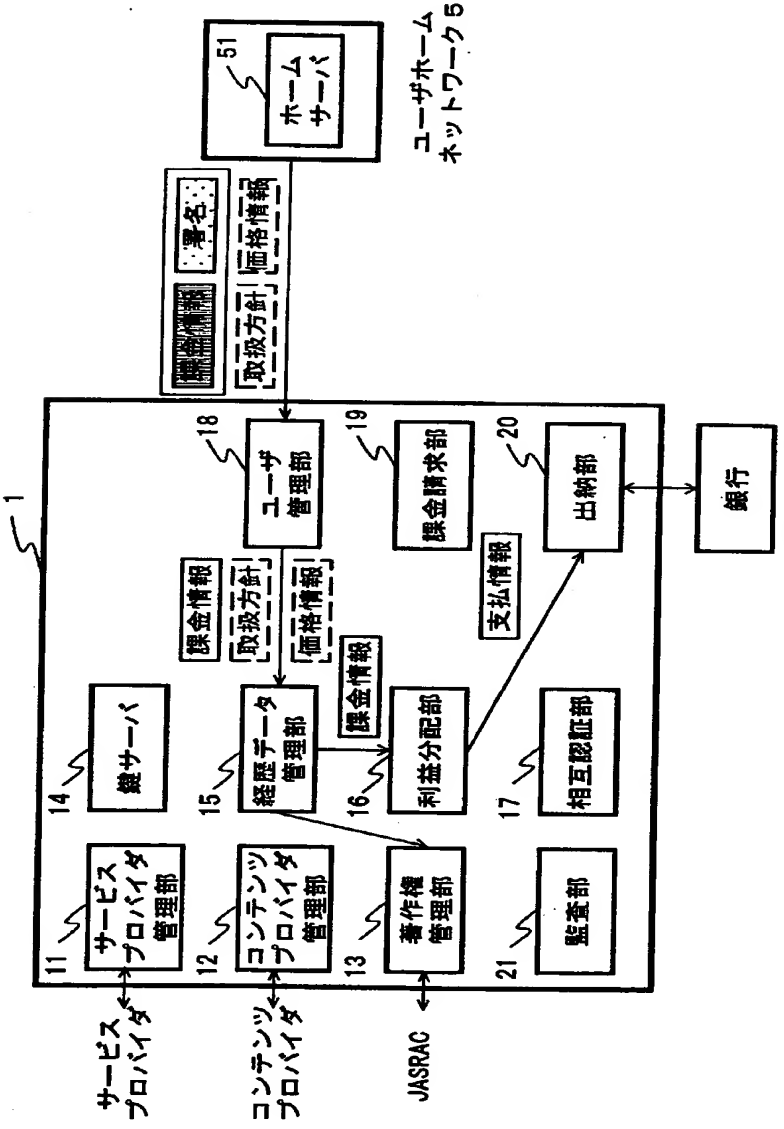


図５５　コンテンツ利用実績の送信動作

【図５６】

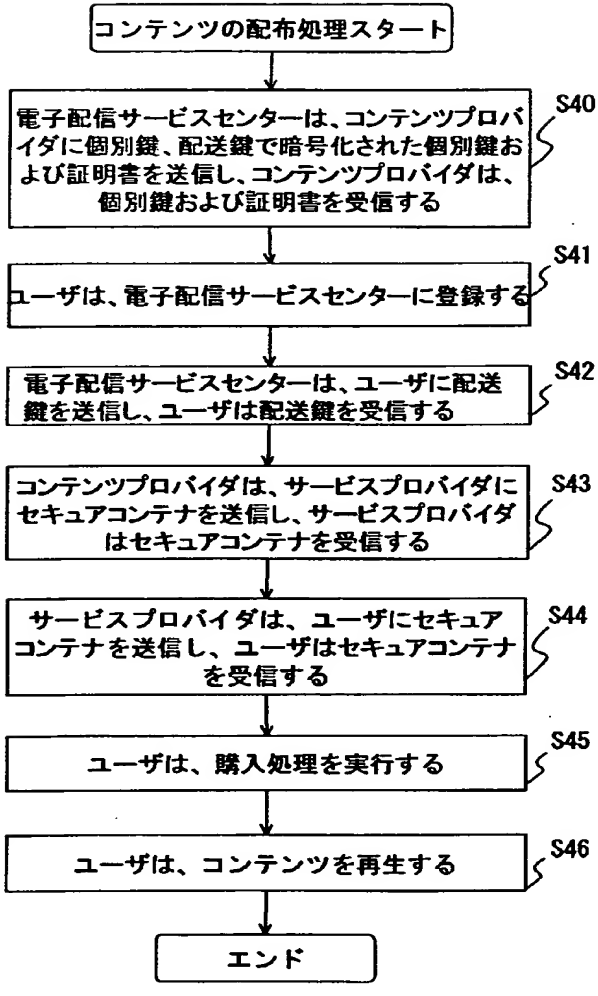


図５６　ＥＤＭシステムのコンテンツ配布、再生処理手順

【図５７】

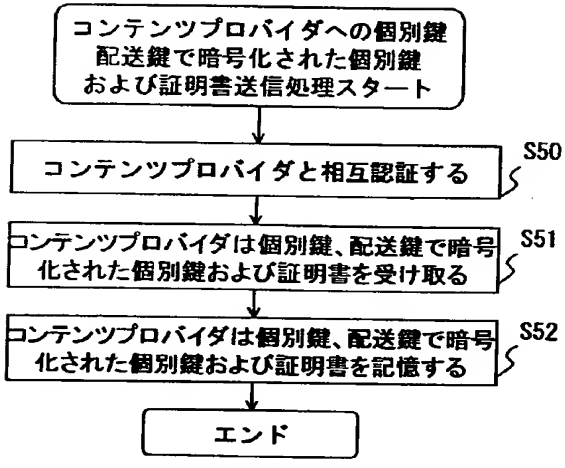


図５７　コンテンツプロバイダへの送信処理手順

【図５８】

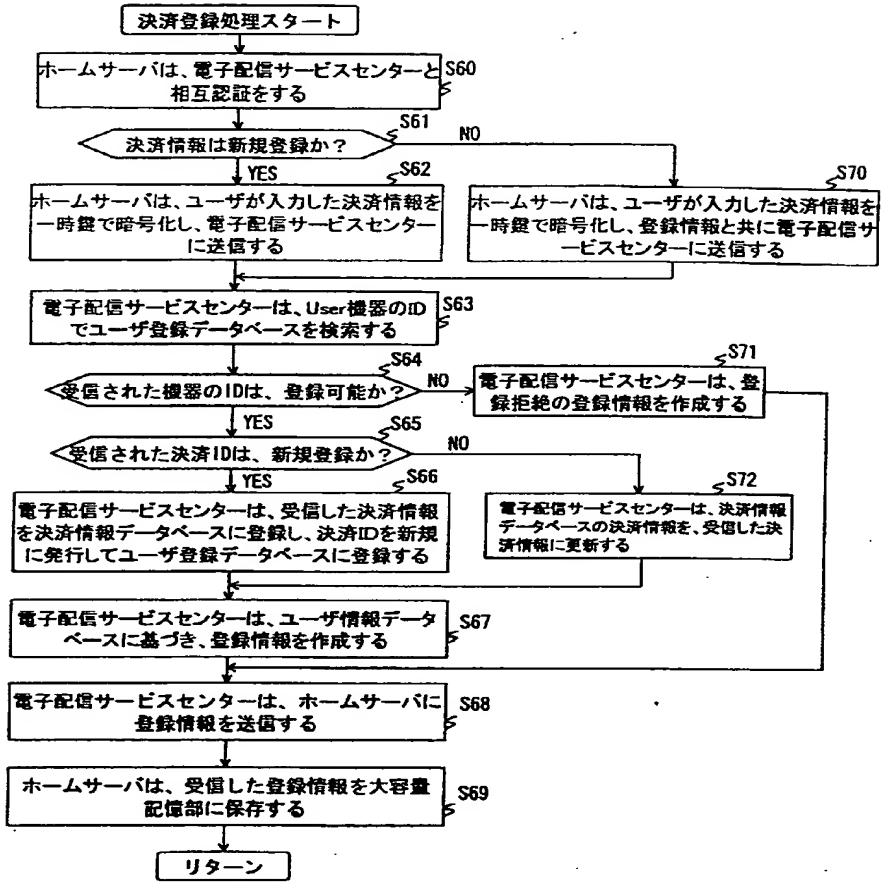


図５８　決済情報の登録処理手順

【図５９】

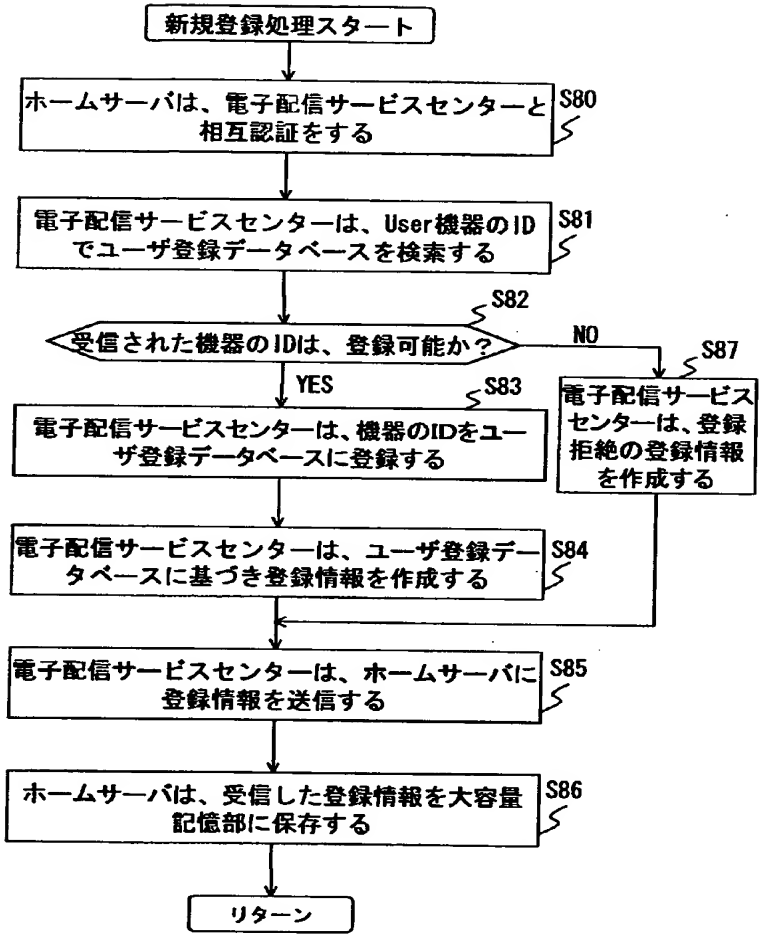


図５９　機器ＩＤの新規登録処理手順

【図６０】

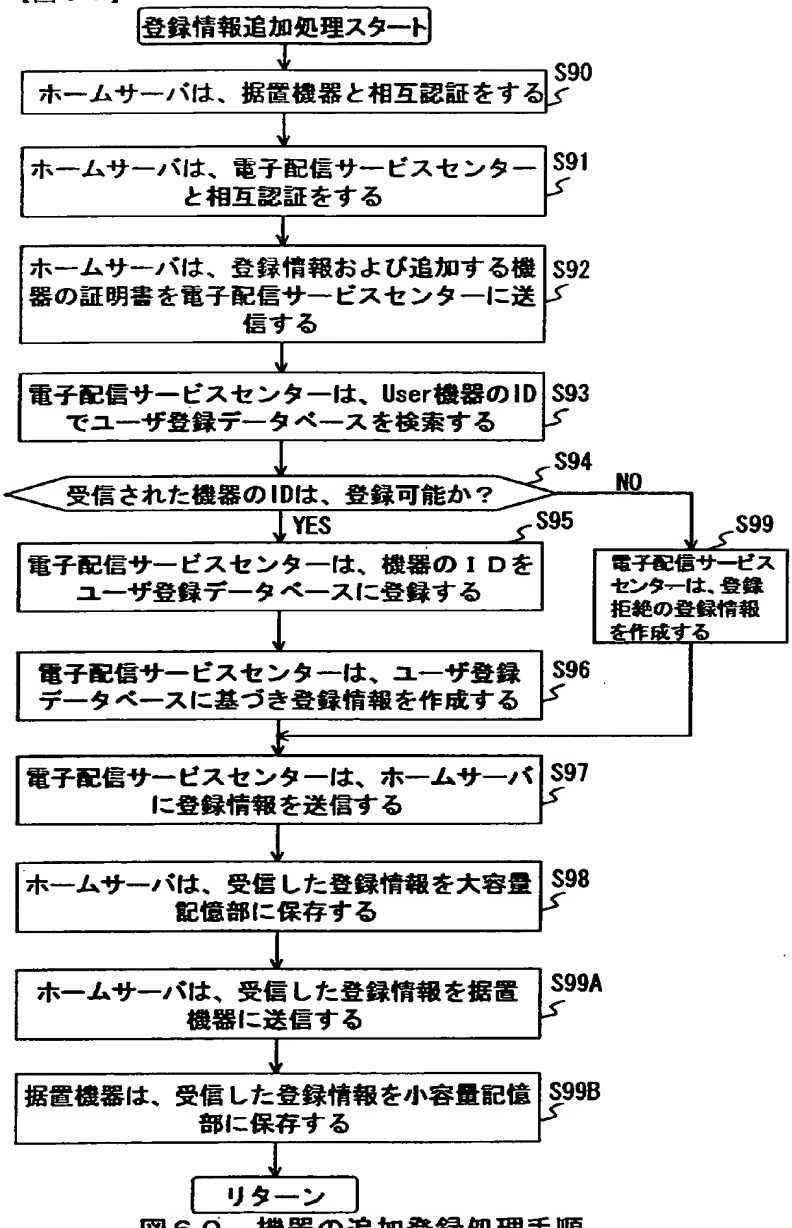


図６０　機器の追加登録処理手順

【図６１】

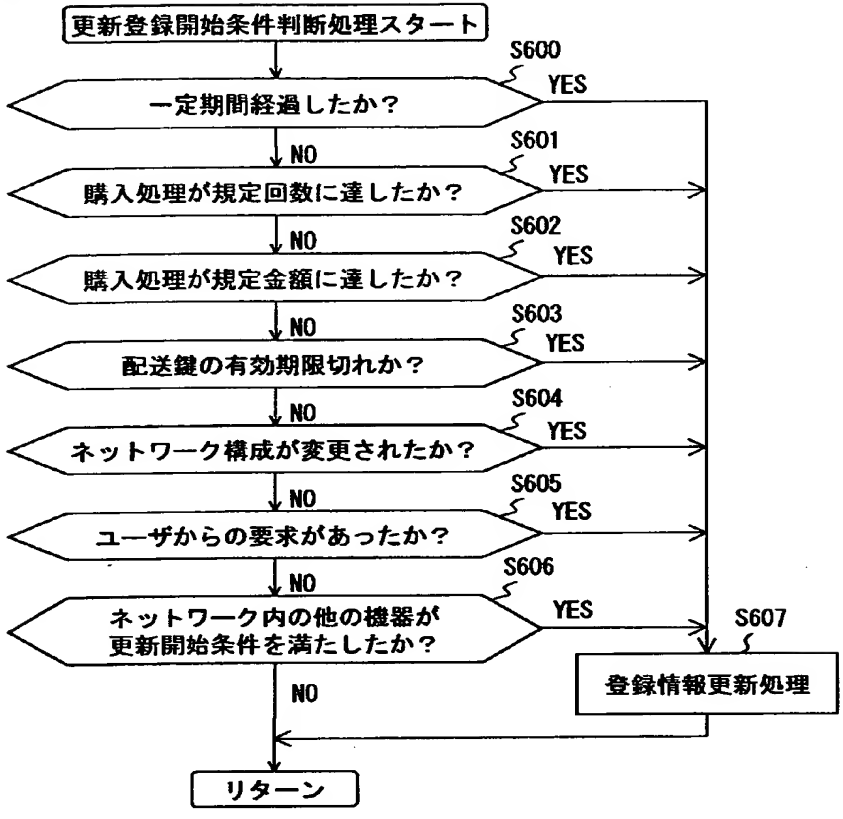


図６１　登録情報の更新開始条件の判断

【図６２】

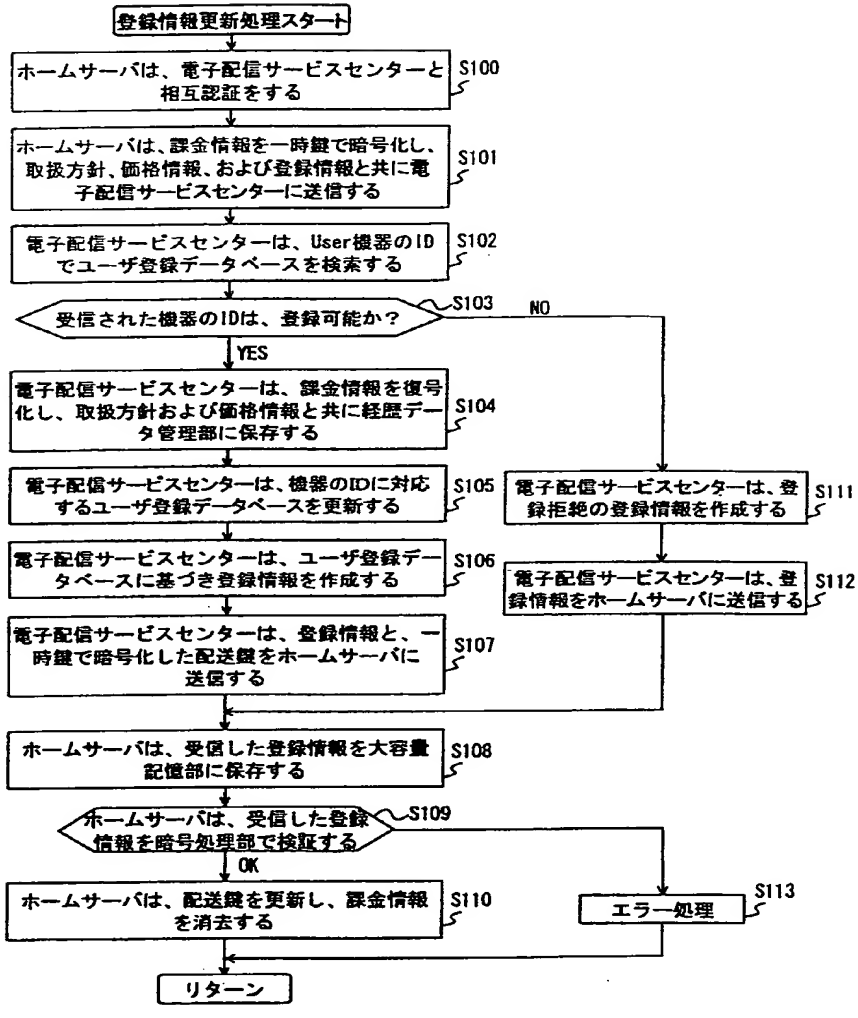


図６２　登録情報更新処理手順

【図６３】

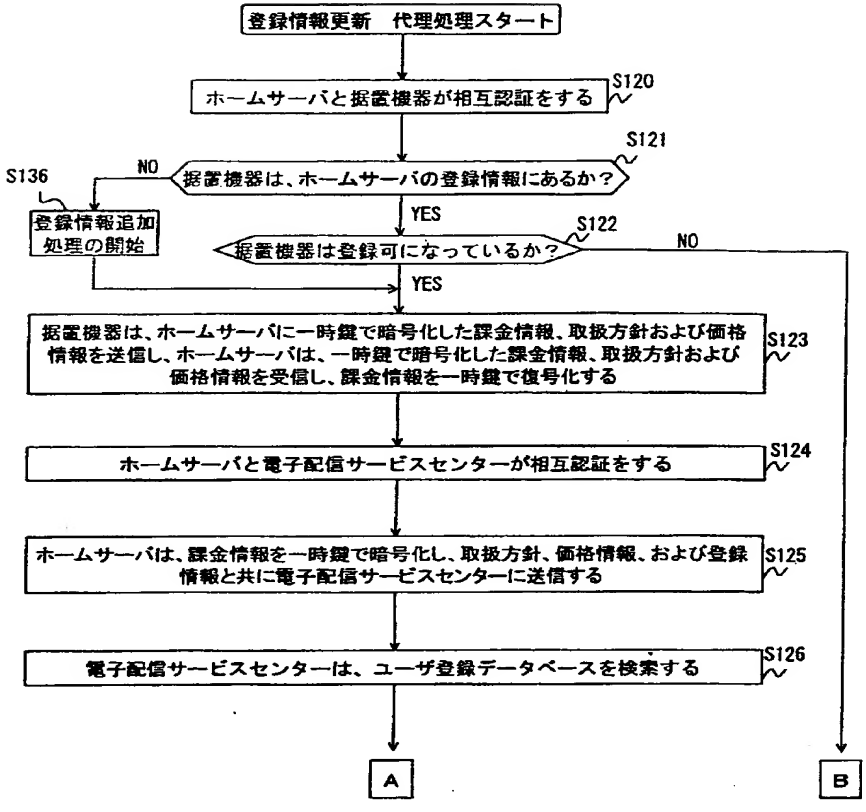


図６３　据え置き機器による登録情報更新代理処理手順（１）

【図６４】

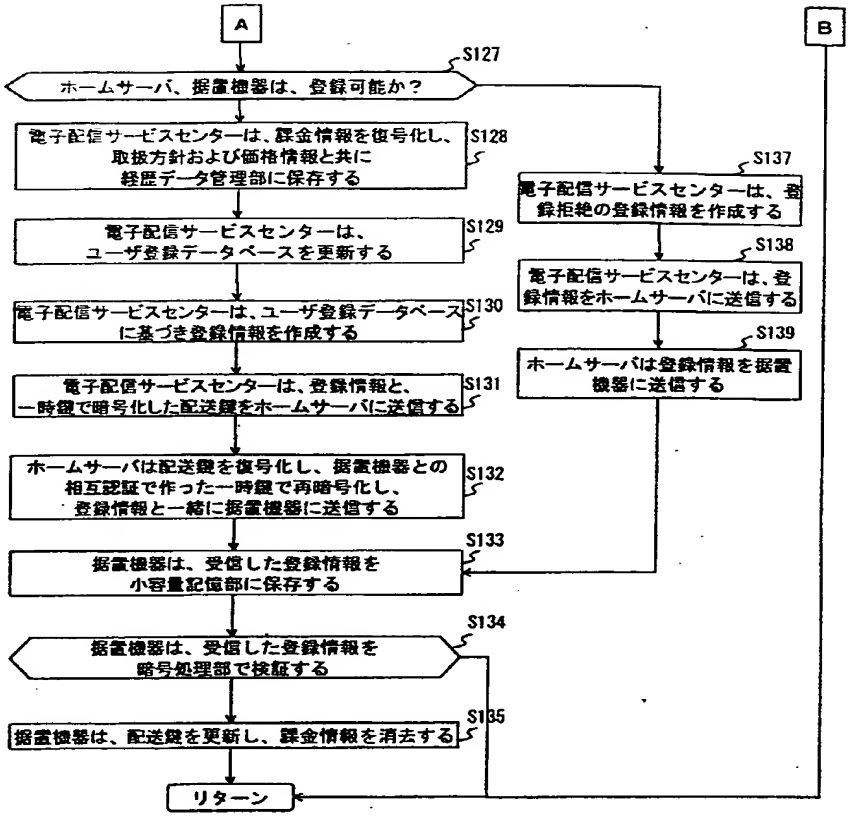


図６４　据え置き機器による登録情報更新代理処理手順（２）

【図６５】

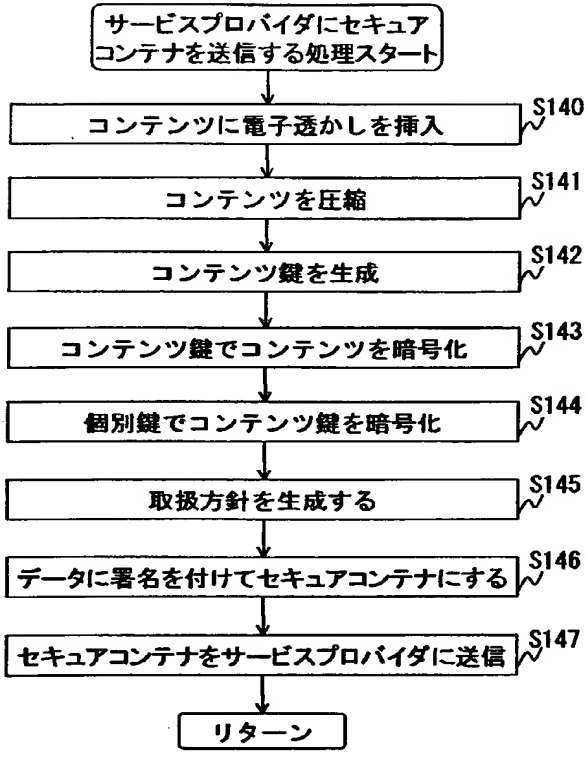


図６５　セキュアコンテナの送信処理手順

【図６６】

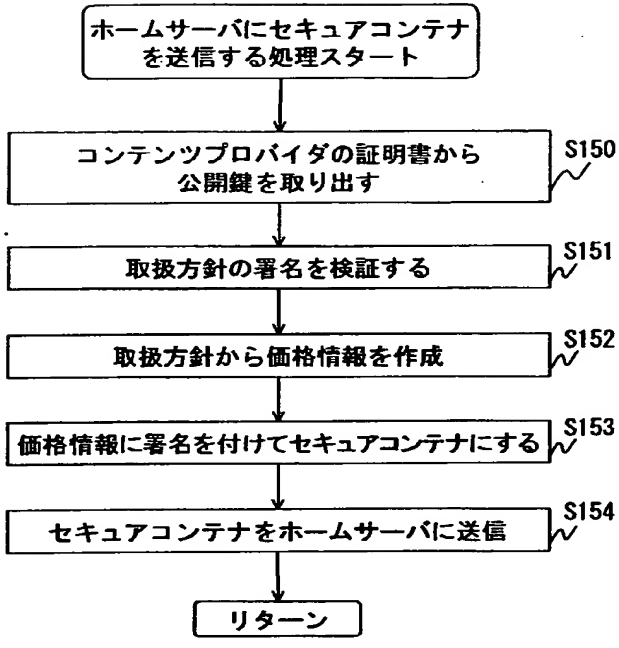


図６６　セキュアコンテナの送信処理手順

【図６７】

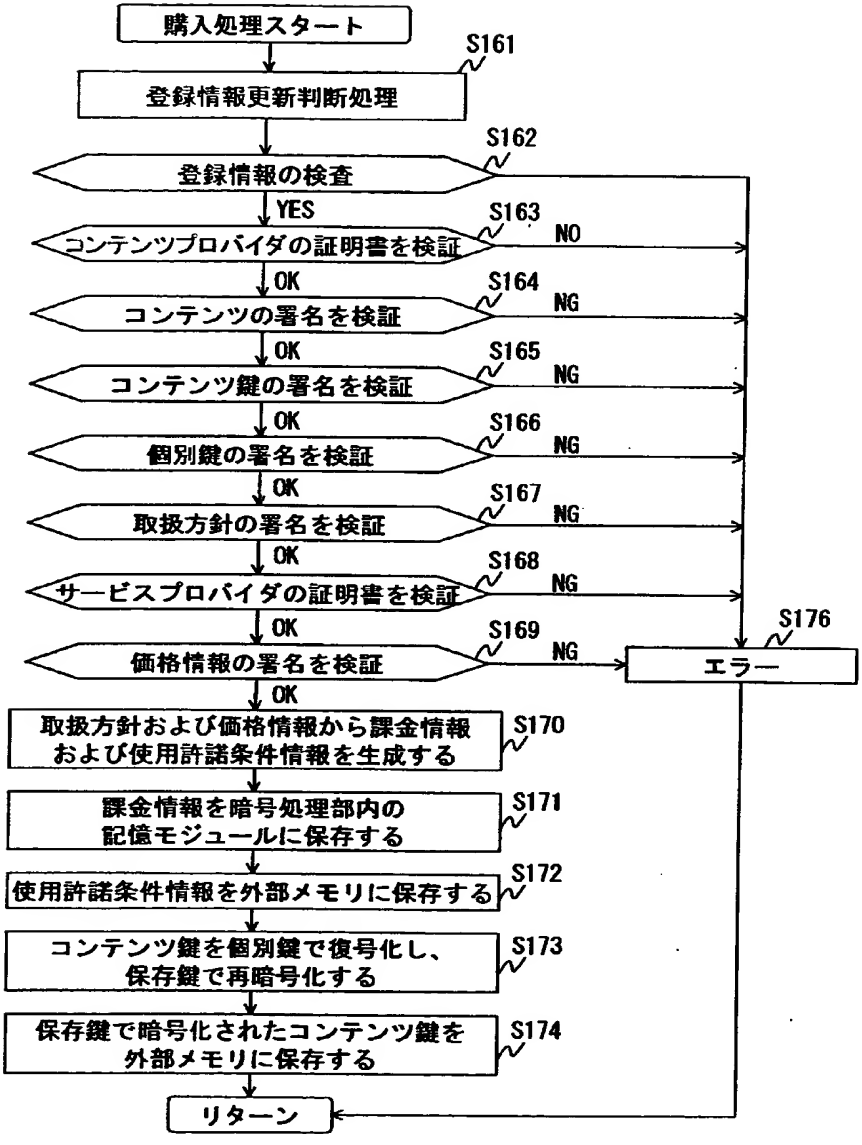


図６７　ホームサーバの購入手順

【図６８】

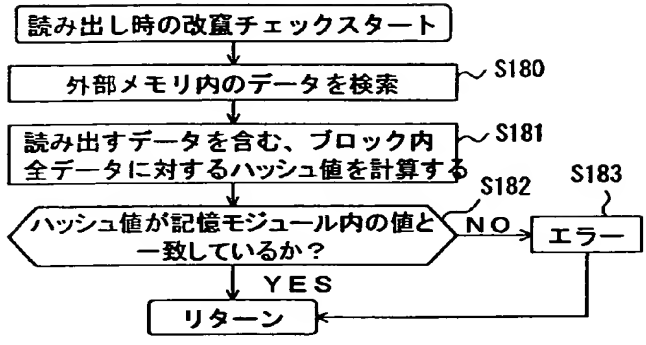


図６８　データ読み出し時の改竄チェック処理手順

【図６９】

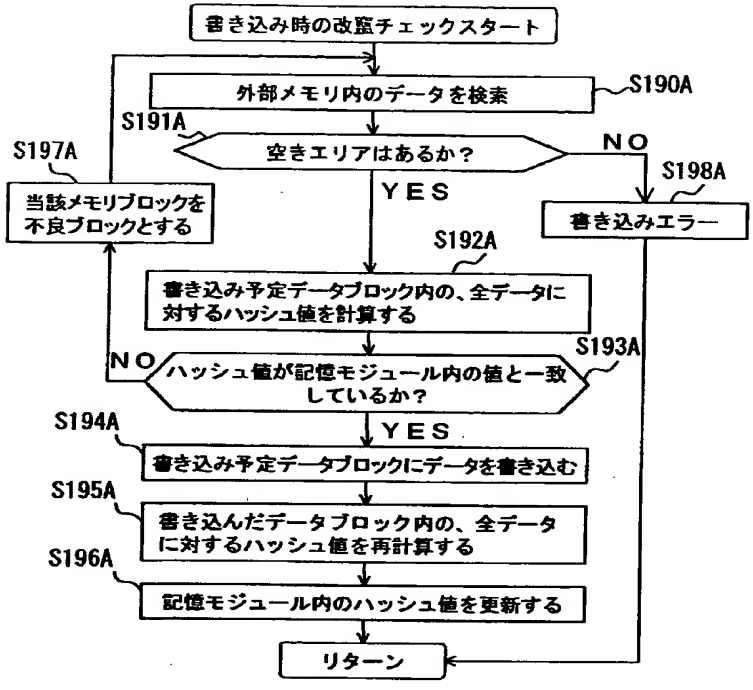


図６９　データ書込み時の改竄チェック処理手順

【図７０】

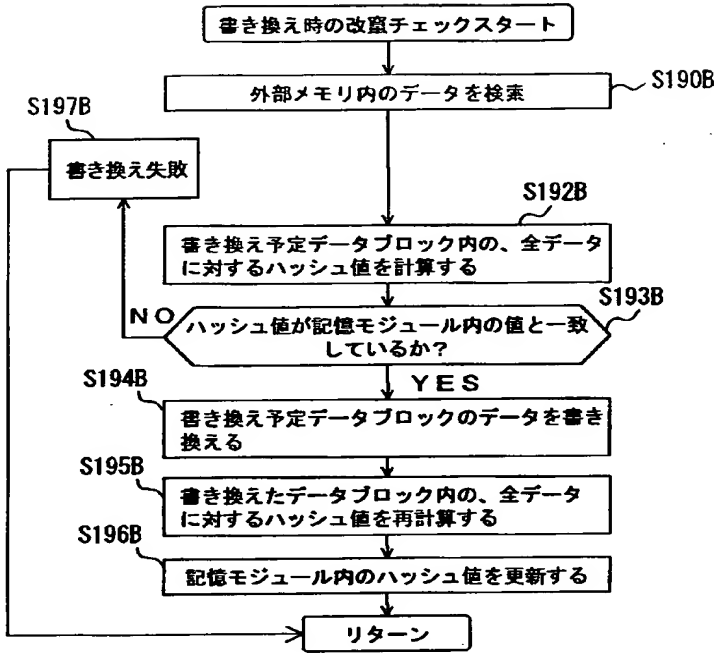


図７０　データ書換え時の改竄チェック処理手順

【図７１】

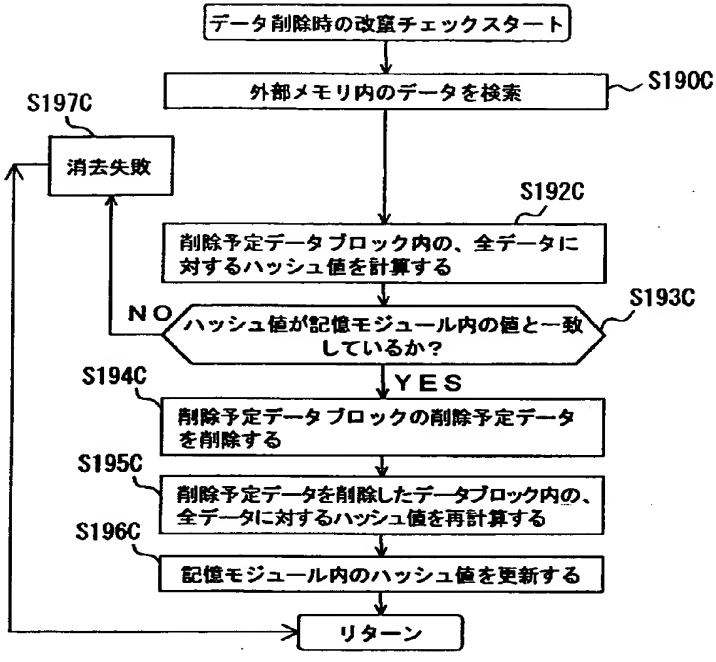


図７１　データ削除時の改竄チェック処理手順

【図７２】

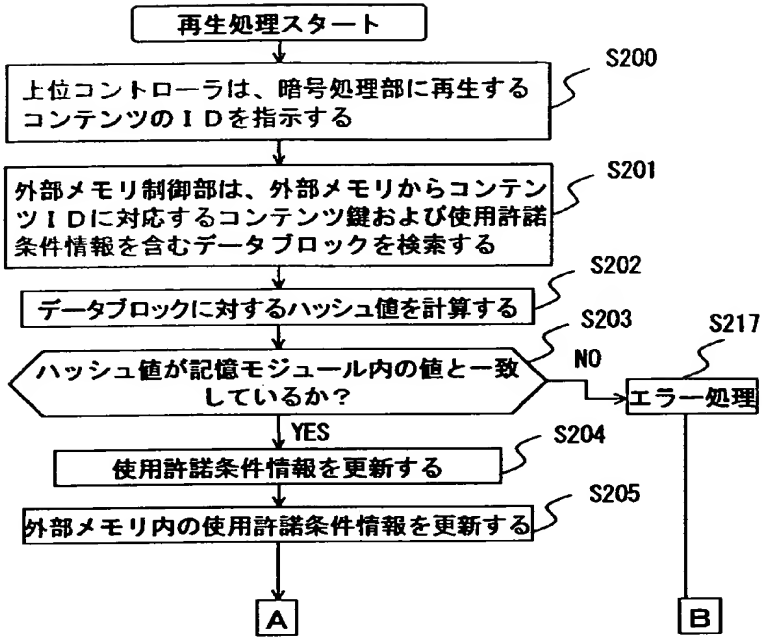


図７２　ホームサーバによるコンテンツの再生処理手順（１）

【図７３】

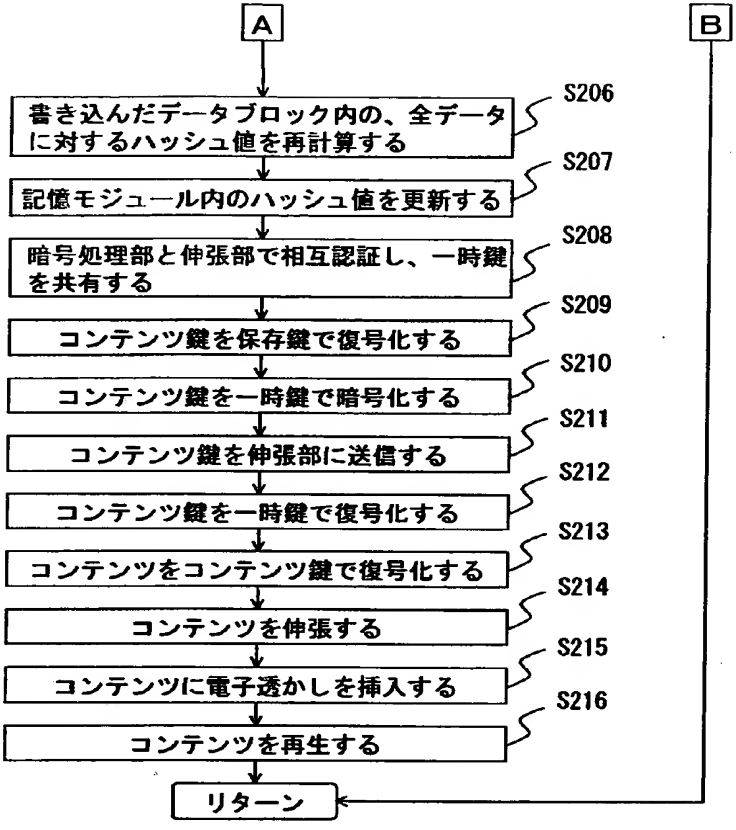


図７３　ホームサーバによるコンテンツの再生処理手順（２）

出証特２０００－３０４９７２６

【図７４】

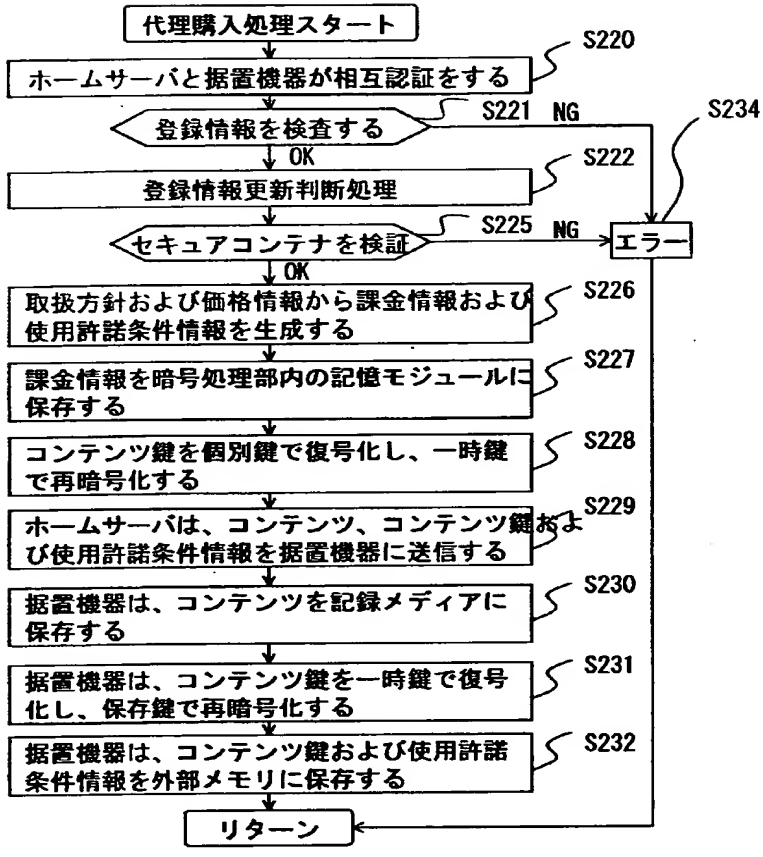


図７４　ホームサーバによるコンテンツ利用権の代理購入処理手順

【図７５】

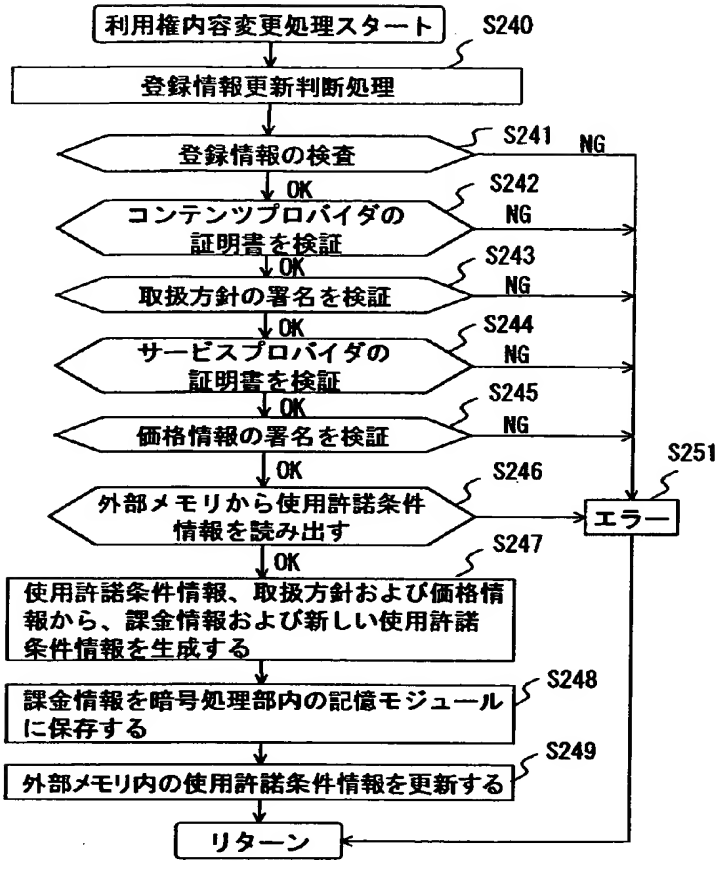


図７５　購入済み利用者の内容変更処理手順

【図７６】

ルールn	ルール番号
	利用権内容番号
	パラメータ
	最低価格
	取り分（利益率）
ルール1	ルール番号＃１
	利用権内容番号　＃１
	なし
	￥３５０
	３０％
ルール2	ルール番号＃２
	利用権内容番号　＃２
	１時間
	￥１００
	３０％
ルール3	ルール番号＃３
	利用権内容番号　＃６
	１回
	￥３０
	３０％
ルール4	ルール番号＃４
	利用権内容番号　＃１３
	＃２／＃１
	￥２００
	２０％
ルール5	ルール番号＃５
	利用権内容番号　＃１４
	＃１／＃１
	￥２５０
	２０％

図７６　取扱方針のルール部の一部

【図７７】

ルールｎ	ルール番号
	パラメータ
	価格
ルール１	ルール番号＃１
	３０％
	￥５００
ルール２	ルール番号＃２
	４０％
	￥１００
ルール３	ルール番号＃３
	４０％
	￥１００
ルール４	ルール番号＃４
	１０％
	￥２００
ルール５	ルール番号＃５
	２０％
	￥３５０

図７７　価格情報のルール部の一部

【図７８】

ルール1	＃１
	＃１
	なし
	￥３５０
	３０％
ルール2	＃２
	＃２
	１時間
	￥１００
	３０％
ルール3	＃３
	＃１３
	＃２／＃１
	￥２００
	２０％

取扱方針のルール部の一部

ルール1	＃１
	３０％
	￥５００
ルール2	＃２
	４０％
	￥１００
ルール3	＃３
	１０％
	￥２００

価格情報のルール部の一部

現在

ルール	ルール番号
	利用権内容番号
	パラメータ
ルール	＃２
	＃２
	３０分／２時間

使用許諾条件情報のルール部

→

変更後

ルール	ルール番号
	利用権内容番号
	パラメータ
ルール	＃１
	＃１
	なし

使用許諾条件情報のルール部

図７８　権利内容の変更例

【図７９】

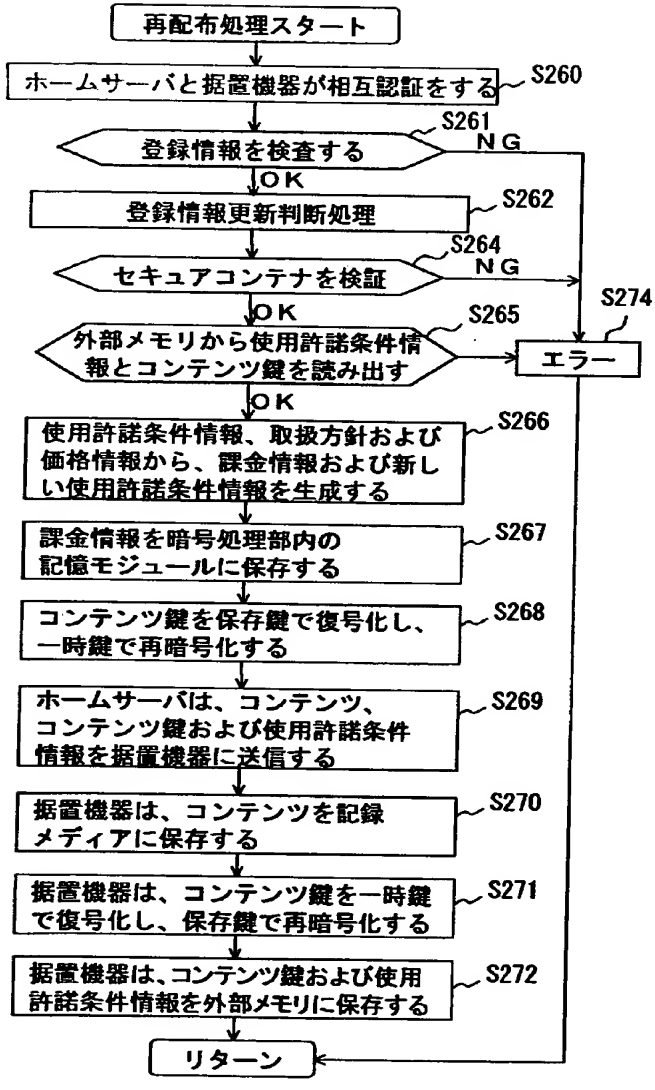


図７９　コンテンツ利用権の再配布処理手順

【図８０】

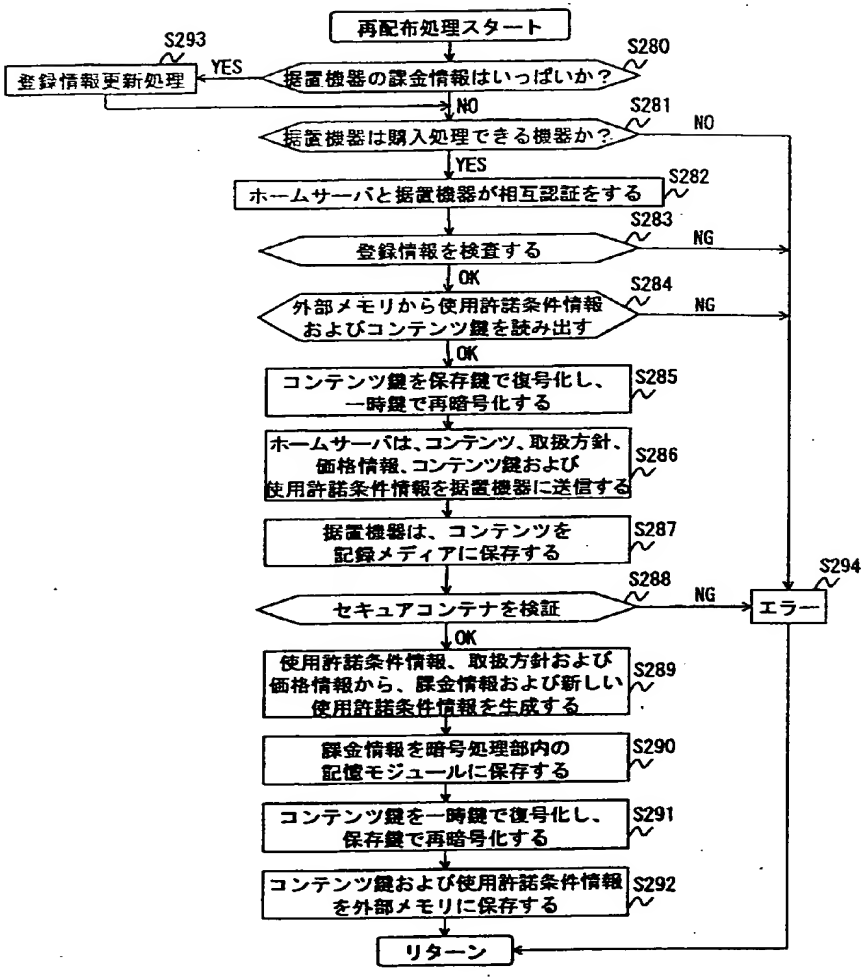


図８０　据置機器でのコンテンツ利用権購入処理手順

【図８１】

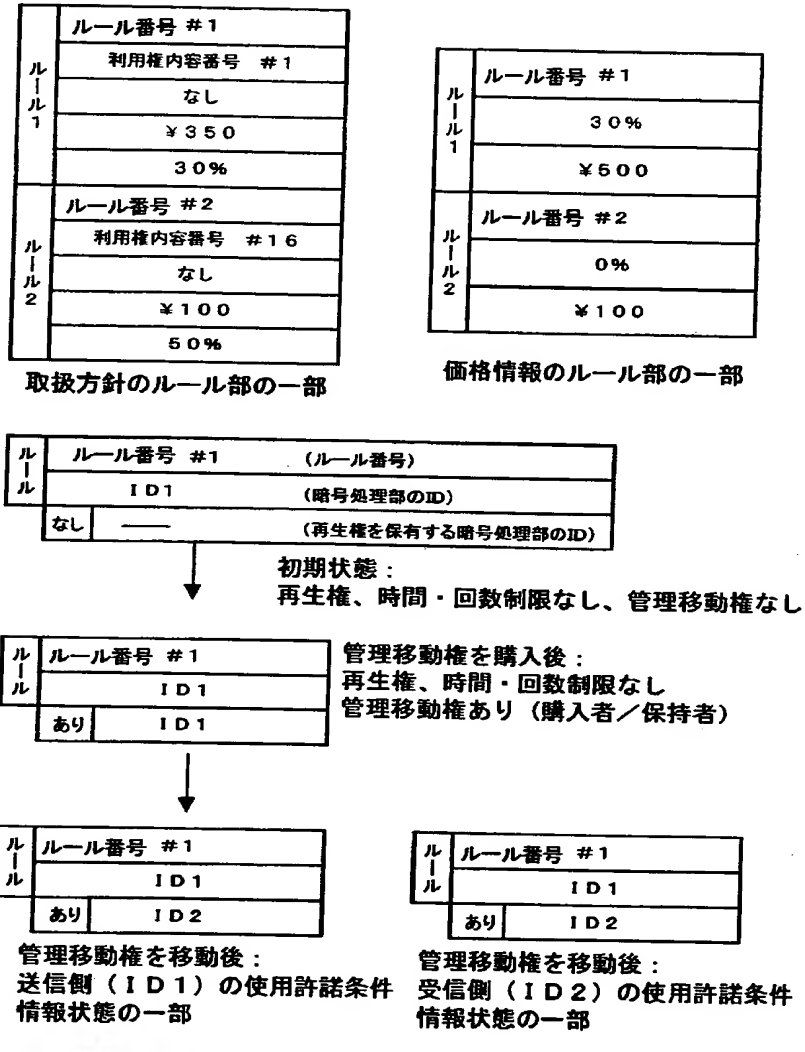


図８１　使用許諾条件情報のルール部の変遷

【図８２】

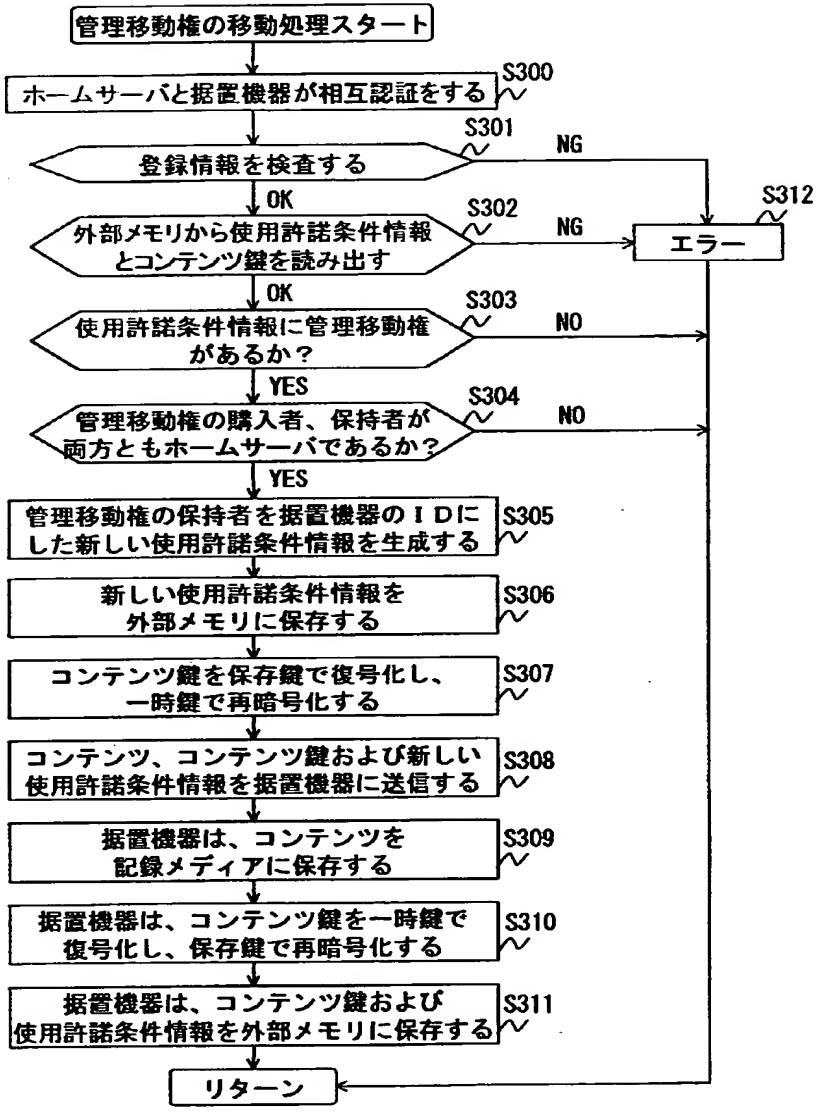


図８２　管理移動権の移動処理手順

【図８３】

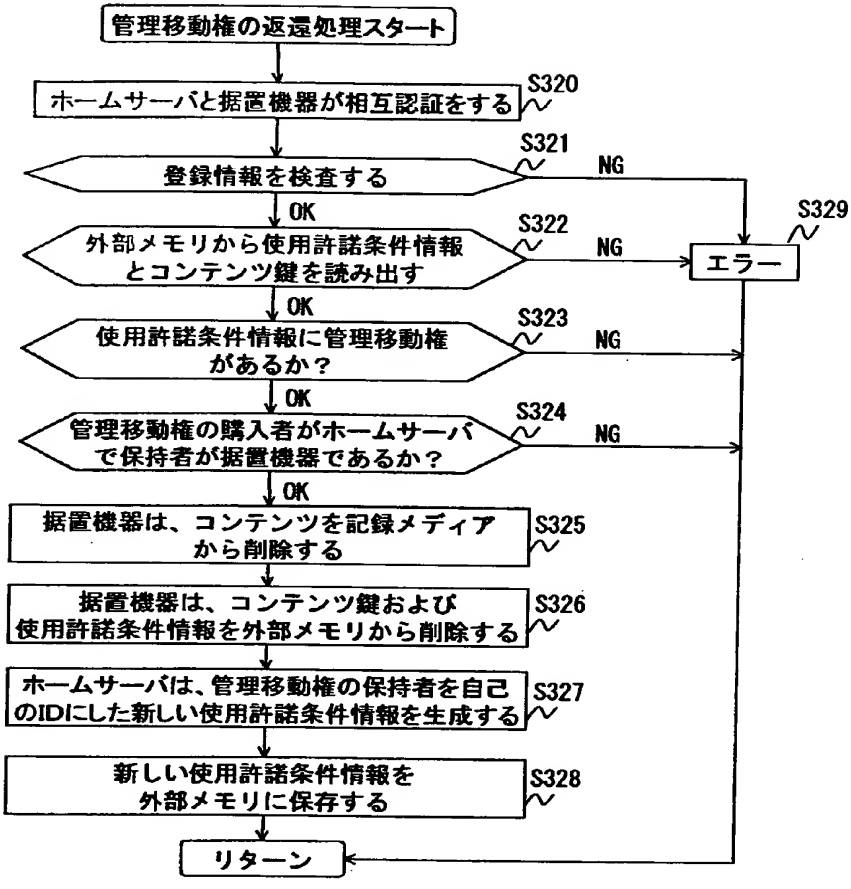


図８３　管理移動権の返還処理手順

【図８４】

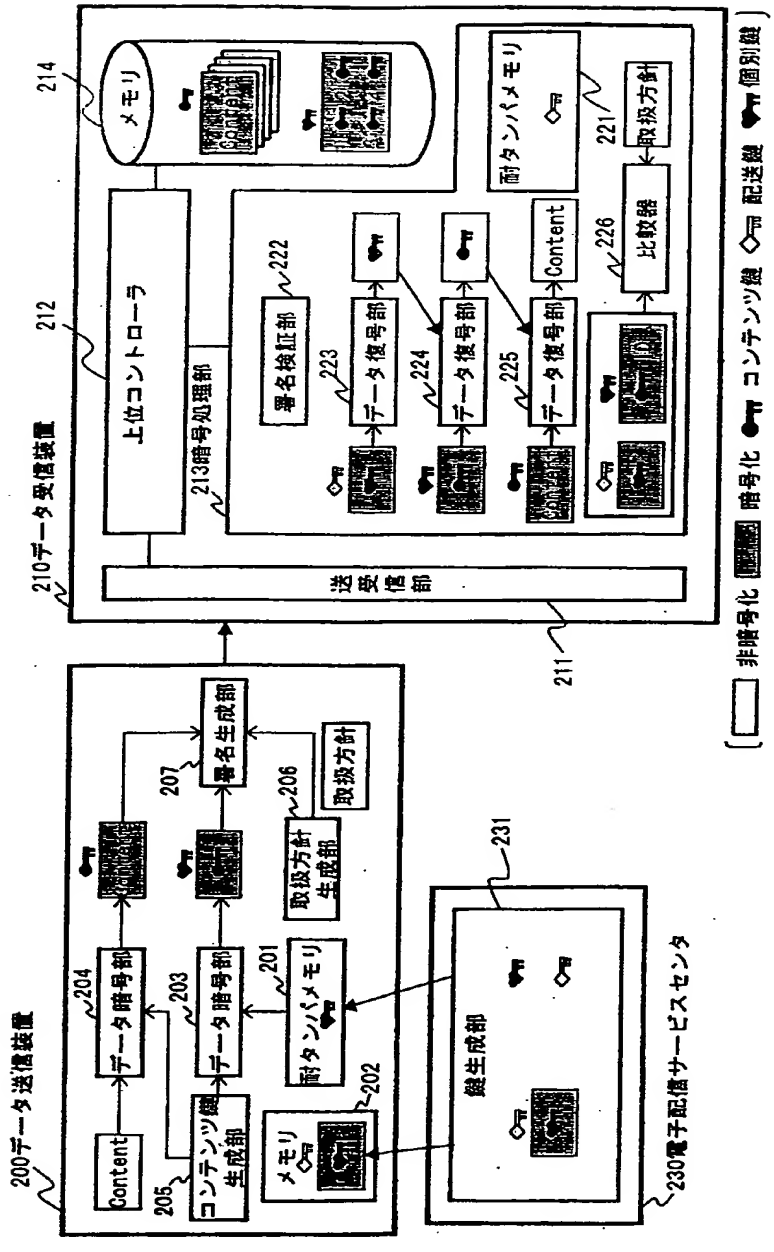


図８４　情報送信システム（１）

【図８５】

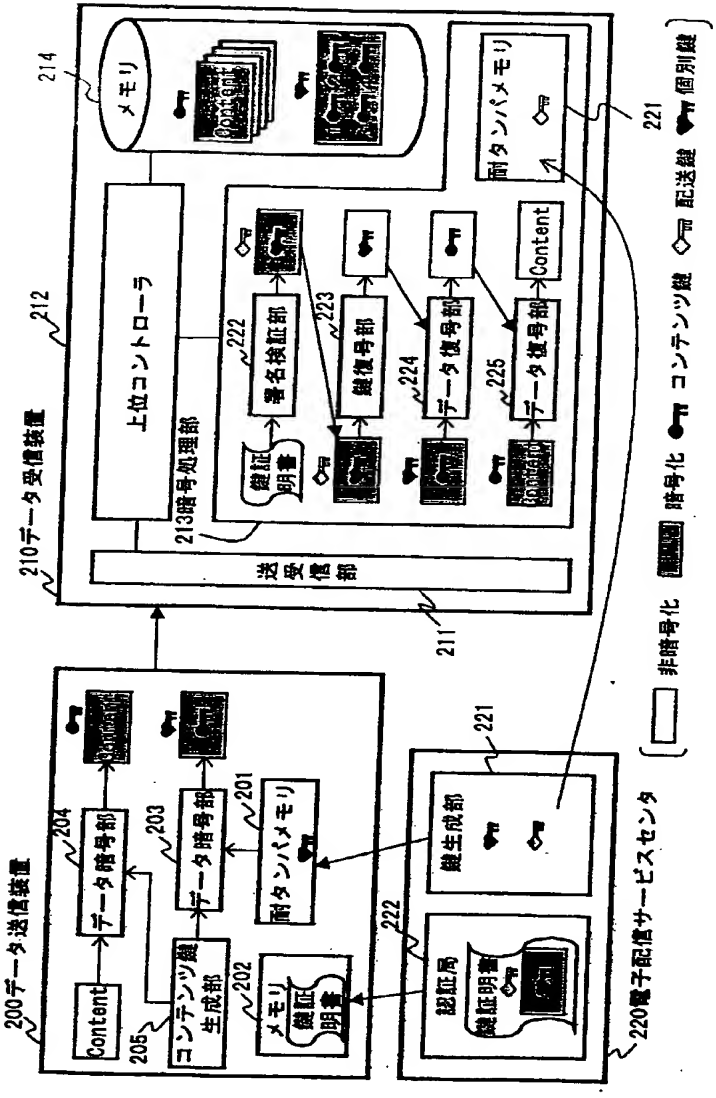


図８５　情報送信システム（２）

【図８６】

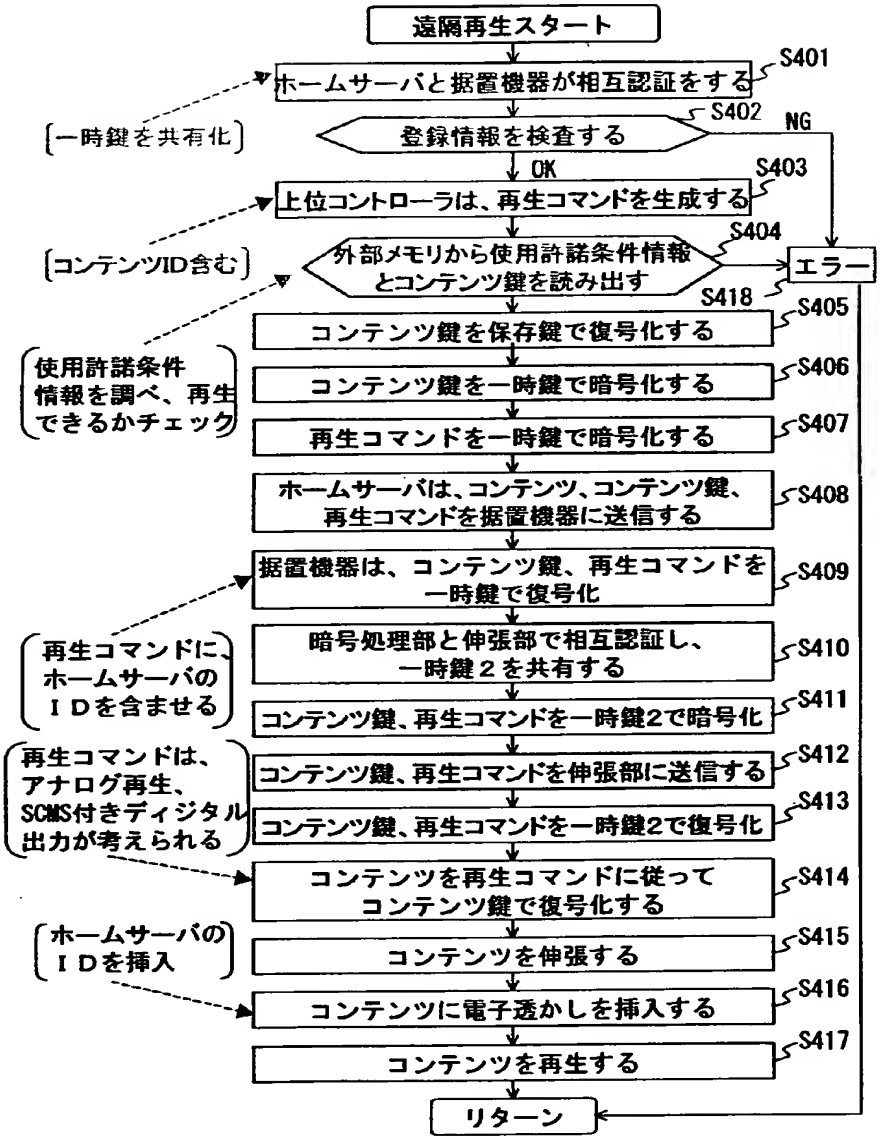


図８６　遠隔再生処理手順

【図８７】

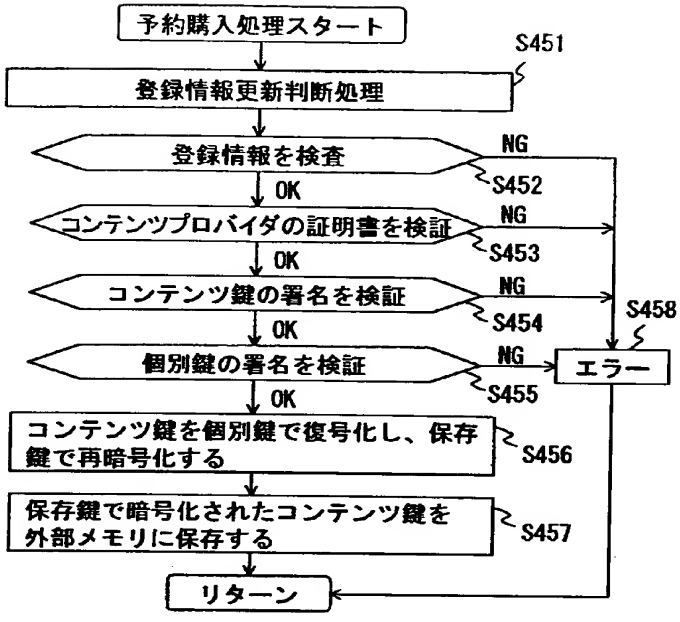


図８７　予約購入処理手順

出証特２０００－３０４９７２６

【図８８】

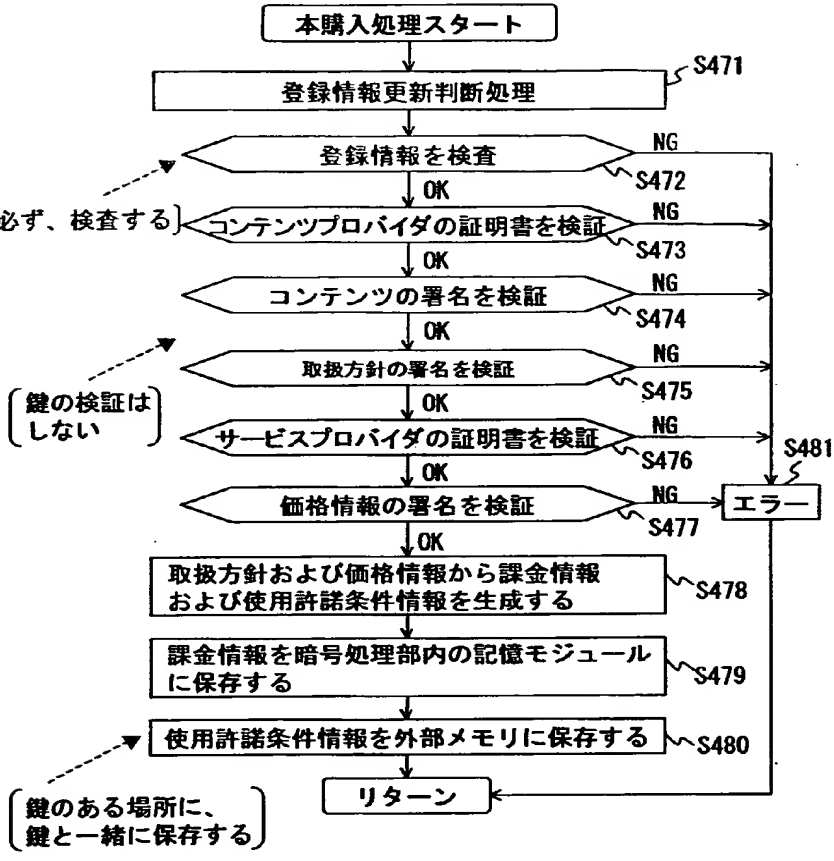


図８８　予約購入後の本購入処理手順

【図８９】

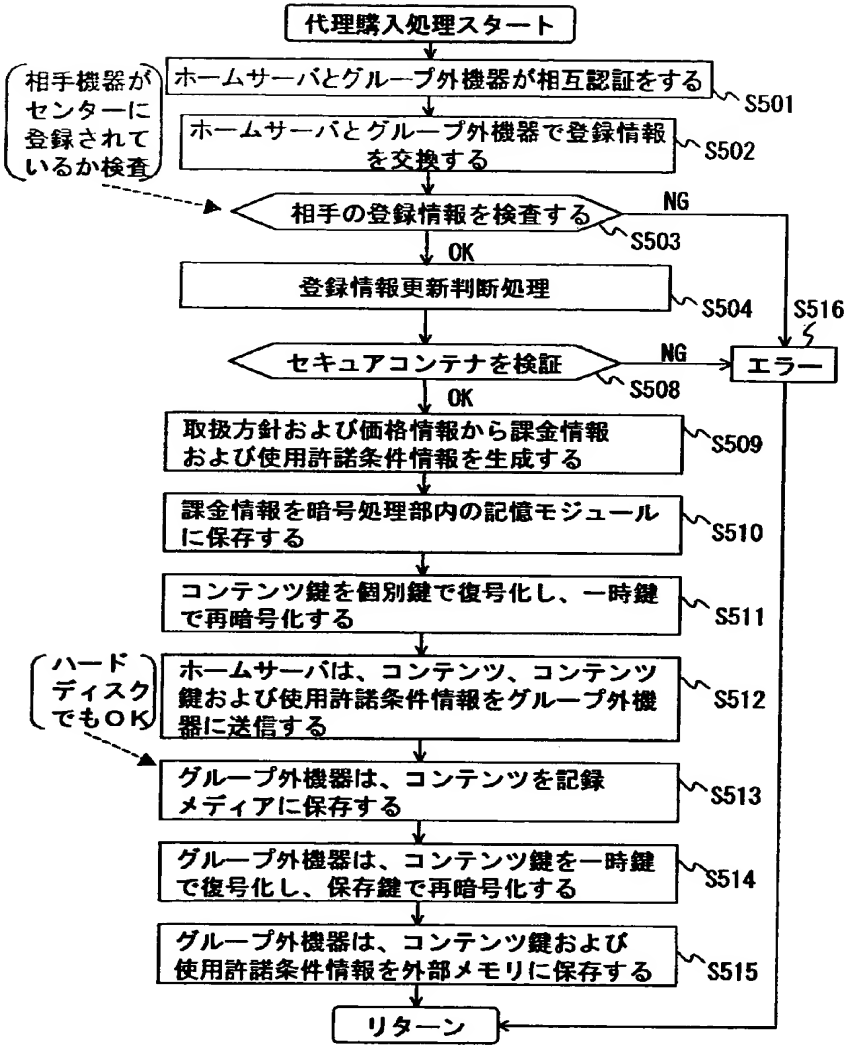


図８９　代理購入処理手順（ホームサーバが支払う場合）

【図９０】

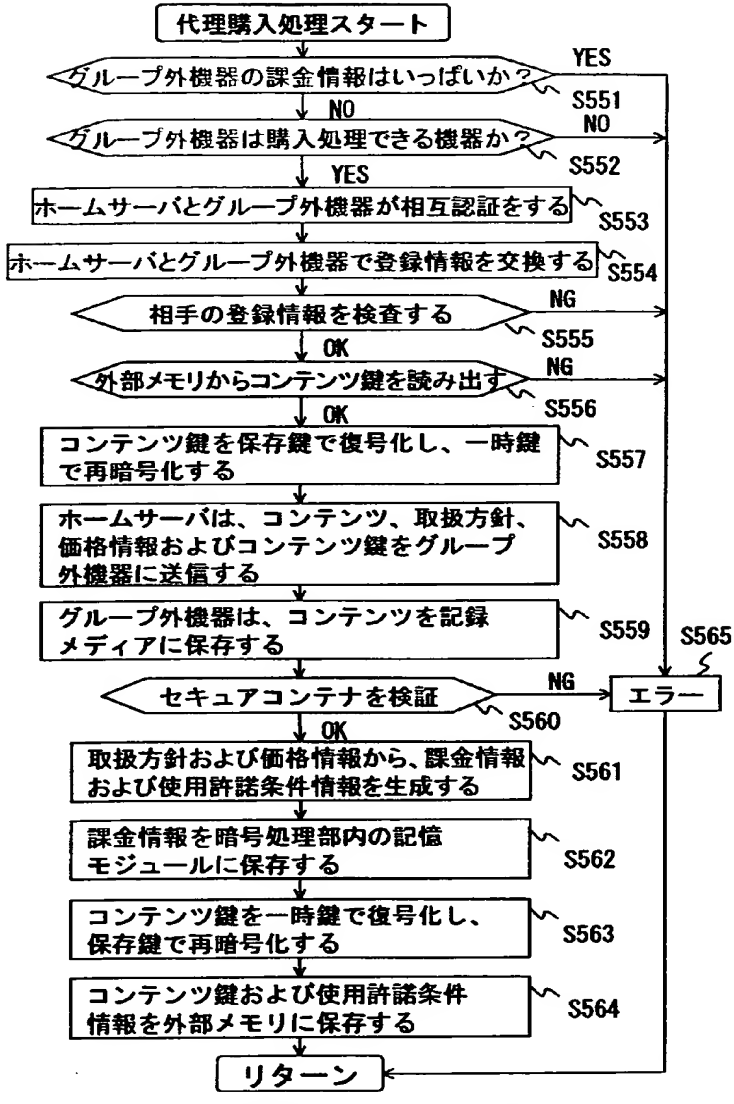


図９０　代理購入処理手順（グループ外機器が支払う場合）

【図９１】

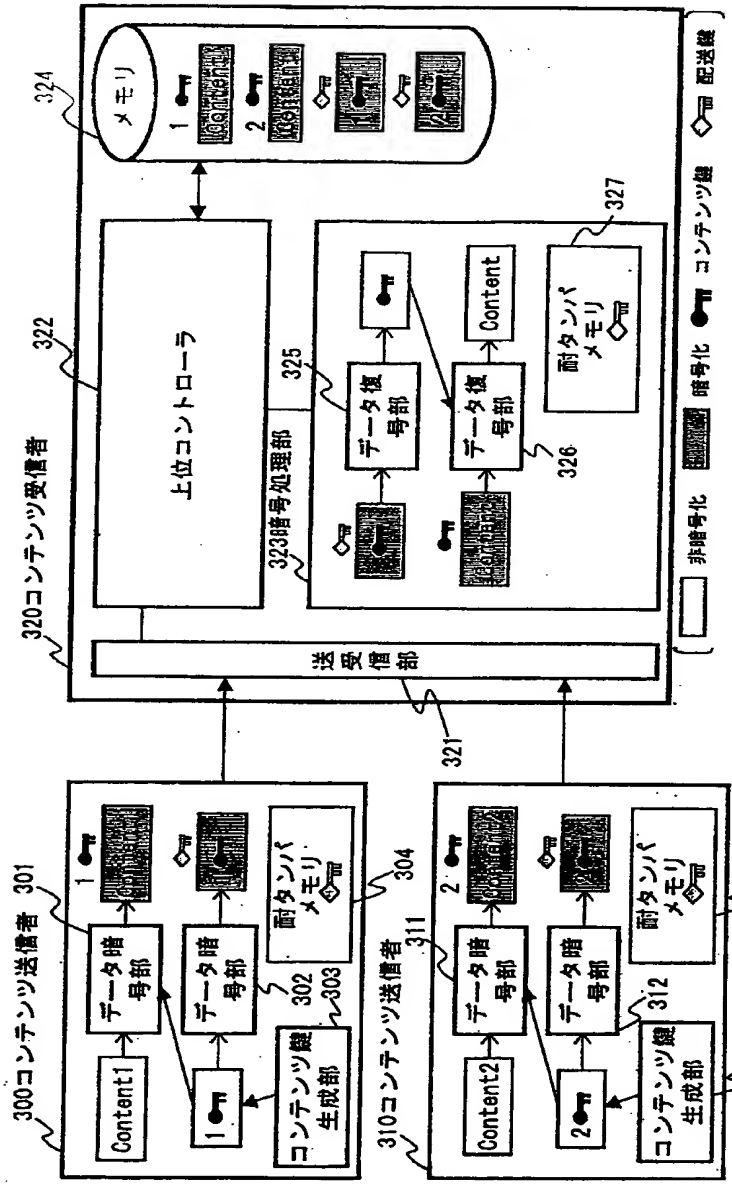

300コンテンツ送信者
301
Content1
1
データ暗号部
データ暗号部
302
コンテンツ鍵生成部
303
耐タンパメモリ
304
310コンテンツ送信者
311
Content2
2
データ暗号部
データ暗号部
312
コンテンツ鍵生成部
313
耐タンパメモリ
314
送受信部
321
320コンテンツ受信者
322
上位コントローラ
323暗号処理部
324
メモリ
Content1
Content2
325
データ復号部
データ復号部
326
Content
耐タンパメモリ
327
非暗号化
暗号化
コンテンツ鍵
配送鍵

図９１　従来例

【書類名】　　要約書

【要約】

【課題】

コンテンツを配信する情報送信システムにおいて、簡易な構成でコンテンツの盗用を防止する。

【解決手段】

コンテンツデータを所定のコンテンツ鍵K_{CO}で暗号化すると共に、情報送信装置固有の個別鍵K_iでコンテンツ鍵K_{CO}を暗号化し、コンテンツ鍵K_{CO}で暗号化されたコンテンツデータと、個別鍵K_iで暗号化されたコンテンツ鍵K_{CO}と、所定の配送鍵K_dで個別鍵K_iを暗号化してなる外部から供給された暗号化個別鍵K_iとを情報受信装置に送信し、情報受信装置は、予め与えられている配送鍵K_dで個別鍵K_iを復号し、当該復号された個別鍵K_iでコンテンツ鍵K_{CO}を復号し、当該復号されたコンテンツ鍵K_{CO}でコンテンツデータを復号する。

複数の情報送信装置は、配送鍵K_dを持たないことにより、互いにコンテンツデータの盗用を防止することができる。そして情報受信装置は、１種類の配送鍵K_dを持つだけで複数の情報送信装置からのコンテンツを復号することができる。

【選択図】　　図８３

出 願 人 履 歴 情 報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社